

CCB Application Notes:

1. Character(s) preceded & followed by these symbols ([␣]␣) or (␣␣) are super- or subscripted, respectively.
EXAMPLES: 42m^{␣3␣} = 42 cubic meters
CO_{␣2␣} = carbon dioxide
2. All degree symbols have been replaced with the word deg.
3. All plus or minus symbols have been replaced with the symbol +/-.
4. All table note letters and numbers have been enclosed in square brackets in both the table and below the table.
5. Whenever possible, mathematical symbols have been replaced with their proper name and enclosed in square brackets.

Naval Facilities Engineering Command
200 Stovall Street
Alexandria, Virginia 22332-2300

APPROVED FOR PUBLIC RELEASE

SN 0525-LP-300-9100

Commercial
Intrusion Detection
Systems
(IDS)

DESIGN MANUAL 13.02
SEPTEMBER 1986

RECORD OF DOCUMENT CHANGES

Instructions: DISCARD THIS SHEET AND NEW RECORD OF DOCUMENT CHANGES SHEET AS ISSUED.

This is an inventory of all changes made to this design manual. Each change is consecutively numbered, and each changed page in the design manual included the date of the change which issued it.

Change Number	Description of Change	Date of Change	Page Changed
------------------	--------------------------	-------------------	-----------------

ABSTRACT

This manual provides guidance for engineering design of Intrusion Detection Systems (IDS) consisting of commercial equipment which is limited to a full range of interior point protection devices, duress sensors, volumetric (space) protection sensors, simple exterior sensors limited to devices that can be attached to perimeter barriers, closed-circuit television for remote alarm assessment purposes, alarm signal data communications media, alarm reporting and monitoring systems, and basic card entry control systems.

FOREWORD

This design manual is one of a series developed from an evaluation of facilities in the shore establishment, from surveys of the availability of new materials and construction methods, and from selection of the best design practices of the Naval Facilities Engineering Command (NAVFACENGCOM), other Government agencies, national professional society, association, and institute standards in accordance with NAVFACENGCOM policy. Deviations from these criteria should not be made without prior approval of NAVFACENGCOM Headquarters (Code 04).

Design cannot remain static any more than the naval functions it serves or the technologies it uses. Accordingly, recommendations for improvement are encouraged from within the Navy and from the private sector and should be furnished to LANTNAVFACENGCOM (Code 04).

This publication is certified as an official publication of NAVFACENGCOM and has been reviewed and approved in accordance with SECNAVINST 5600.16 Series, "Procedures Governing Review of Department of the Navy (DN) Publications."

J. P. JONES, JR.
Rear Admiral, CEC, U. S. Navy
Commander
Naval Facilities Engineering Command

SECURITY ENGINEERING AND DESIGN

<u>Number</u>	<u>Title</u>	<u>PA</u>	<u>Date</u>
DM-13.01	Physical Security	NCEL	Mar 1983
DM-13.02	Commercial Intrusion Detection Systems (IDS)	L	Dec 1985

COMMERCIAL INTRUSION DETECTION SYSTEMS (IDS)

CONTENTS

	<u>Page</u>
 Section 1 INTRODUCTION	
1.1	Scope..... 13.02-1
1.2	Related Criteria..... 13.02-1
1.3	How to Use This Manual..... 13.02-2
1.3.1	Organization and Application of This Manual.... 13.02-2
 Section 2 ELEMENTS OF INTRUSION DETECTION SYSTEMS	
2.1	Introduction..... 13.02-3
2.1.1	System Integration..... 13.02-3
2.2	Security Subsystems Overview..... 13.02-3
2.3	Barrier/Delay Subsystem..... 13.02-3
2.3.1	Barrier/Delay Subsystem Elements..... 13.02-5
2.4	Detection Subsystem..... 13.02-6
2.4.1	Detection Subsystem Elements..... 13.02-6
2.5	Assessment Subsystem..... 13.02-9
2.5.1	Assessment Subsystem Elements..... 13.02-9
2.6	Access Control Subsystem..... 13.02-11
2.6.1	Access Control Subsystem Elements..... 13.02-11
2.7	Related Subsystems..... 13.02-13
2.7.1	Personnel and Equipment Subsystem..... 13.02-13
2.7.2	Procedures Subsystem..... 13.02-13
2.8	Summary..... 13.02-13
 Section 3 BASICS OF SECURITY SYSTEM DESIGN	
3.1	Introduction..... 13.02-15
3.2	Facility Categorization..... 13.02-15
3.2.1	Factors Influencing System Design Criteria..... 13.02-15
3.2.2	Facility Sensitivity/Criticality..... 13.02-16
3.2.3	Threat and Consequences of Events..... 13.02-17
3.3	Specific Requirements of DoD and Navy Directives..... 13.02-17
3.4	Basic System Design Considerations..... 13.02-17
3.4.1	Know the Environment..... 13.02-17
3.4.2	Provide for Protection-in-Depth..... 13.02-20
3.4.3	Provide for High Probability of Detection and Low Nuisance Alarm Rates..... 13.02-20
3.4.4	Design for Cost-Effectiveness..... 13.02-21
3.4.5	Flexibility and Expansion..... 13.02-21
3.4.6	Build the Detection Subsystem for Point-for-Point Annunciation..... 13.02-21
3.4.7	Build the System for Ease of Operation and Maintenance..... 13.02-21
3.4.8	Provide for Critical Area Sensor Zones to be Tied Into CCTV Assessment..... 13.02-22
3.4.9	Integrate Security Subsystems for Total Protection..... 13.02-22

	Page
3.5	Security System Design Process..... 13.02-22
3.5.1	NAVFAC Responsibility for Security Requirements Analysis..... 13.02-22
3.5.2	Consistency of the Security System and MCON Design Process..... 13.02-22
3.5.3	Phase 1 - Requirements Definition..... 13.02-23
3.5.4	Phase 2 - Development of Preliminary System Design..... 13.02-25
3.5.5	Phase 3 - Preparation of Final System Design... 13.02-27
3.5.6	Phase 4 - System Implementation..... 13.02-29

Section 4 TYPES OF SENSORS

4.1	Point Sensors - Interior..... 13.02-32
4.1.1	Door and Window Protection..... 13.02-32
4.1.2	Object Protection..... 13.02-38
4.1.3	Floor, Wall, and Ceiling Protection..... 13.02-40
4.2	Volumetric Sensors - Interior..... 13.02-43
4.2.1	Infrared Sensors..... 13.02-43
4.2.2	Ultrasonic Sensors..... 13.02-46
4.2.3	Microwave Sensors..... 13.02-48
4.2.4	Audio Sensors..... 13.02-49
4.2.5	Photoelectric Sensors..... 13.02-50
4.2.6	CCTV - Motion Detection..... 13.02-50
4.2.7	Interior Sensor Summary..... 13.02-52
4.3	Exterior Fence Sensors..... 13.02-52
4.3.1	Electromechanical Fence Sensors..... 13.02-59
4.3.2	Strain Sensitive Cable..... 13.02-60
4.3.3	Electrostatic Field Fence Sensors..... 13.02-61
4.3.4	Taut Wire Sensors..... 13.02-63
4.3.5	Balanced Magnetic Gate Switch (BMS)..... 13.02-65
4.3.6	Barrier Protection..... 13.02-65
4.3.7	Exterior Fence Sensor Summary..... 13.02-66
4.4	Duress Alarms..... 13.02-66
4.4.1	Hardwire Duress Alarms..... 13.02-67
4.4.2	Radio Frequency Duress Alarms..... 13.02-67
4.4.3	Other Approaches to Duress..... 13.02-67

Section 5 BASIC AUTOMATED ACCESS CONTROL

5.1	Importance of Access Control to Security Operations..... 13.02-69
5.1.1	Increased Use of Automated Access Control in Security Operations..... 13.02-69
5.1.2	Electronic Access Control Requires Effective Planning..... 13.02-69
5.2	Components of Automated Access Control Systems. 13.02-69
5.2.1	Coded Badge..... 13.02-70
5.2.2	Badge Reader..... 13.02-73
5.2.3	Electric Door Locks..... 13.02-75
5.2.4	Remote (Control) Units..... 13.02-76
5.2.5	Central Control Unit..... 13.02-77

	Page
	<hr/>
5.3	Automated Access Control System Functions..... 13.02-78
5.3.1	Access Authorization/Verification and Reporting..... 13.02-78
5.3.2	Area Authorization..... 13.02-78
5.3.3	Time Zoning..... 13.02-78
5.3.4	Fail Safe/Fail Soft..... 13.02-79
5.3.5	Occupant Listing..... 13.02-79
5.3.6	Anti-Passback..... 13.02-79
5.3.7	Security Enhancement..... 13.02-79
5.4	Modularity - Building in Expansion and Growth.. 13.02-80
5.5	Considerations for Application and Installation..... 13.02-80
 Section 6 REMOTE ALARM ASSESSMENT	
6.1	The Role of CCTV in Security Operations..... 13.02-82
6.1.1	Near Real Time Alarm Assessment..... 13.02-82
6.1.2	Alarm Response Direction..... 13.02-83
6.1.3	Directed Surveillance..... 13.02-83
6.1.4	Event Recording..... 13.02-83
6.1.5	Access Monitoring..... 13.02-83
6.2	Components of Basic Closed-Circuit Systems..... 13.02-84
6.2.1	Cameras..... 13.02-84
6.2.2	Lenses..... 13.02-87
6.2.3	Monitors..... 13.02-90
6.2.4	Options for Enhanced Capabilities..... 13.02-92
6.2.5	The Role of Lighting in CCTV Effectiveness..... 13.02-98
 Section 7 ALARM SIGNAL COMMUNICATIONS	
7.1	Criticality of Communications in System Integrity..... 13.02-103
7.2	Types of Communications Links..... 13.02-103
7.2.1	Hardwire/Landline..... 13.02-103
7.2.2	Proprietary Installations..... 13.02-107
7.2.3	Telephone Line to On- or Off-Site..... 13.02-108
7.2.4	Radio Frequency..... 13.02-108
7.2.5	Microwave..... 13.02-108
7.2.6	Fiber Optics..... 13.02-109
7.3	Remote (Control) Units..... 13.02-109
7.4	Line Security Techniques..... 13.02-111
7.4.1	Line Supervision..... 13.02-111
7.4.2	Physical Protection of System Components..... 13.02-111
7.4.3	Environmentally Generated Interference..... 13.02-113
 Section 8 ALARM REPORTING AND DISPLAY	
8.1	Intrusion Detection System Integration..... 13.02-115
8.2	Locating the Alarm Control Function..... 13.02-115
8.2.1	Threat Considerations..... 13.02-115
8.2.2	Termination Options..... 13.02-115
8.2.3	On-Site Location..... 13.02-118
8.2.4	Off-Site Location..... 13.02-119
8.2.5	Redundancy Considerations..... 13.02-120
8.3	Using Existing Equipment..... 13.02-121

		Page
8.4	Reporting and Display System Components.....	13.02-122
8.4.1	Annunciator Units.....	13.02-122
8.4.2	Status Control.....	13.02-123
8.4.3	Hard Copy Output.....	13.02-124
8.4.4	Visual Reporting.....	13.02-125
8.5	Conclusions.....	13.02-127

Section 9 POTENTIAL SYSTEM CONFIGURATIONS AT GENERIC NAVY FACILITIES

9.1	Introduction.....	13.02-129
9.2	Aircraft Hangar.....	13.02-130
9.2.1	Perimeter.....	13.02-130
9.2.2	Interior.....	13.02-130
9.2.3	Alarm Reporting and Display.....	13.02-130
9.3	Communications Facility (Exclusion Area).....	13.02-132
9.3.1	Automated Access Control.....	13.02-132
9.3.2	Detection.....	13.02-132
9.3.3	Assessment.....	13.02-132
9.4	Supply Warehouse.....	13.02-134
9.4.1	Detection.....	13.02-134
9.4.2	Assessment.....	13.02-134
9.4.3	Control.....	13.02-134
9.5	Funds and Negotiable Instrument Storage Area...	13.02-136
9.5.1	Detection.....	13.02-136
9.5.2	Assessment.....	13.02-136
9.6	Intrusion Detection System Monitoring Area.....	13.02-138
9.6.1	Detection.....	13.02-138
9.6.2	Assessment.....	13.02-138
9.7	BX Retail Area.....	13.02-140
9.7.1	Perimeter.....	13.02-140
9.7.2	Interior.....	13.02-140
9.7.3	Control and Annunciation.....	13.02-140
9.7.4	Assessment.....	13.02-140
9.8	Commissary Retail Area.....	13.02-142
9.8.1	Detection.....	13.02-142
9.8.2	Alarm Reporting and Display.....	13.02-142
9.8.3	Assessment.....	13.02-142
9.9	Command Quarters.....	13.02-144
9.9.1	Detection.....	13.02-144
9.9.2	Alarm Reporting and Display.....	13.02-144
9.10	Sensitive Compartmented Information Facility (SCIF).....	13.02-146
9.10.1	Access Control.....	13.02-146
9.10.2	Detection.....	13.02-146
9.10.3	Assessment.....	13.02-146
9.11	Navy and Marine Corps Reserve Facility.....	13.02-148
9.11.1	Detection.....	13.02-148
9.11.2	Alarm Reporting and Display.....	13.02-148
9.12	Training Facilities.....	13.02-150
9.12.1	Access Control.....	13.02-150

	Page
	<hr/>
9.12.2	Detection..... 13.02-150
9.12.3	Alarm Reporting and Display..... 13.02-150
9.13	Automated Data Processing Facility..... 13.02-152
9.13.1	Access Control..... 13.02-152
9.13.2	Detection..... 13.02-152
9.13.3	Assessment..... 13.02-152
 Section 10 INTRUSION DETECTION SYSTEMS SITE SURVEY GUIDE	
10.1	Purpose..... 13.02-154
10.1.1	Classification of Completed Guides..... 13.02-154
10.1.2	Relationship of Checklist to Applicable Directives..... 13.02-154
10.1.3	Project Complexity..... 13.02-154
10.2	Using This Guide in Conjunction with the Design Manual..... 13.02-154

APPENDICES

APPENDIX A, Design Symbolology

FIGURES

1	Relationship of DM-13.02 to MCON Implementation Process...	13.02-2
2	Security Subsystem Options.....	13.02-4
3	Barrier/Delay Subsystem.....	13.02-5
4	Detection Subsystem.....	13.02-7
5	Detection Subsystem Communications & Control.....	13.02-8
6	System Support and Performance Elements.....	13.02-9
7	Assessment Subsystem Elements.....	13.02-10
8	Access Control Subsystem Elements.....	13.02-11
9	Security Personnel & Equipment Subsystem.....	13.02-14
10	Phase 1 - Requirements Definition.....	13.02-23
11	Vulnerability Analysis Process.....	13.02-25
12	Phase 2 - Preliminary System Design.....	13.02-26
13	Phase 3 - Final System Design.....	13.02-27
14	Phase 4 - System Implementation.....	13.02-29
15	Standard Magnetic Switch Application.....	13.02-33
16	Standard Magnetic Switch Application (Enlarged View).....	13.02-33
17	Vibration/Ultrasonic Glass Breakage Sensor Application....	13.02-37
18	Capacitance Proximity Sensor Application.....	13.02-39
19	Vibration Sensor (Wall/Floor/Ceiling Protection).....	13.02-41
20	Grid Wire Sensor Application.....	13.02-42
21	Passive Infrared Sensor Coverages.....	13.02-44

	Page
22	Ultrasonic Sensor Coverages..... 13.02-47
23	Microwave Sensor Coverages..... 13.02-48
24	CCTV Motion Detection Sensor Image..... 13.02-51
25	Electromechanical Fence Sensor..... 13.02-59
26	Strain Sensitive Cable Sensor..... 13.02-61
27	Electrostatic Field Sensor..... 13.02-62
28	Taut Wire Fence Sensor Applications..... 13.02-64
29	Block Diagram Access Control..... 13.02-71
30	Components of the Basic CCTV System..... 13.02-84
31	Camera Tube Geometry and Formats..... 13.02-85
32	Lens Relative Fields of View..... 13.02-89
33	Tilt and Pan Motions..... 13.02-93
34	Camera Housings and Enclosures..... 13.02-94
35	Homing Sequential Switchers..... 13.02-99
36	Bridging Sequential Switchers..... 13.02-99
37	Looping Sequential Switchers..... 13.02-100
38	Looping/Bridging Sequential Switchers..... 13.02-100
39	Natural and Artificial Light Source Versus Camera Tube Sensitivities..... 13.02-102
40	Normally Closed (N.C.) Circuit..... 13.02-104
41	Normally Open (N.O.) Circuit..... 13.02-104
42	Typical Local Hardware IDS Communications Configuration... 13.02-105
43	Direct Wire Hookup (CCTV)..... 13.02-106
44	Remote (Control) Unit..... 13.02-110
45	End-of-Line (EOL) Circuit Design..... 13.02-111
46	Dual EOL Resistance Circuit Design..... 13.02-112
47	Short Occurring on "Hot Loop" Design..... 13.02-112
48	Example of Short Occurring on "End-of-Line" or "Return Circuit Design"..... 13.02-112
49	Protected Circuits..... 13.02-113
50	Integrated Facility Control System..... 13.02-116
51	Relationship of the IDS Alarm Reporting and Display Function to Other Security System Components..... 13.02-120
52	Microprocessor-Based Reporting and Control System..... 13.02-127
53	Integrated Physical Protection System..... 13.02-128
54	Sensor Symbols..... 13.02-129
55	Aircraft Hangar..... 13.02-131
56	Communications Facility (Exclusion Area)..... 13.02-133
57	Supply Warehouse..... 13.02-135
58	Funds and Negotiable Instrument Storage Area..... 13.02-137
59	Intrusion Detection System Monitoring Area..... 13.02-139
60	B.X. Retail Area..... 13.02-141
61	Commissary Retail Area..... 13.02-143
62	Command Quarters..... 13.02-145
63	Sensitive Compartmented Information Facility (SCIF)..... 13.02-147
64	Navy and Marine Corps Reserve Facility..... 13.02-149
65	Training Facilities..... 13.02-151
66	Automated Data Processing Facility/Area..... 13.02-153

TABLES

1	Facility Categorization by Criticality.....	13.02-16
2	Range of Threats and Consequences.....	13.02-18
3	DoD and Navy Physical Security Directives.....	13.02-19
4	Interior Sensor Summary.....	13.02-53
5	Space Protection - Detector Selection.....	13.02-55
6	Motion Sensor Survey Checklist.....	13.02-58
7	Summary of Exterior Fence Sensors.....	13.02-66
8	Card Access Guidelines.....	13.02-81
9	Source Light Level Variations and Applicable Camera Tubes.	13.02-86
10	Camera Cost Comparison.....	13.02-88
11	Lens Application Guide.....	13.02-91
12	Monitor Size Selection.....	13.02-92
13	Sequential Switcher Definitions.....	13.02-97
14	Switcher Selection Guide.....	13.02-101
15	CCTV Coaxial Cable Characteristics.....	13.02-106
16	Protective Techniques for Alarm Communication Links.....	13.02-109
17	Typical Alarm Loop Lengths.....	13.02-110
18	Alarm System Termination Options.....	13.02-117

BIBLIOGRAPHY

REFERENCES.....	13.02-193
-----------------	-----------

Section 1: INTRODUCTION

1.1 Scope. This design manual provides guidance for Naval Facilities Engineering Command (NAVFACENGCOM) personnel involved in the analysis, design, engineering and/or implementation of intrusion detection systems (IDS) at Department of the Navy shore-based installations. Coverage of IDS elements in this manual is limited to commercially available equipment including the range of interior point protection devices, duress alarms, interior space protection sensors, simple exterior sensors limited to devices that can be attached to perimeter barriers, closed-circuit television for remote alarm assessment purposes, alarm signal data communication media, alarm reporting and monitoring systems, and basic card access control systems. This manual is applicable to shore-based facilities within the 50 United States (except nuclear storage and conventional Arms, Ammunition and Explosives (AA&E) sites) for which Commander, Naval Facilities Engineering Command (COMNAVFACENGCOM) has Military Construction (MCON) design responsibility for commercial IDS systems.

1.2 Related Criteria. Several agencies of DOD and the Department of the Navy have cognizant responsibility for issuance of policy, directives, guidance, or other criteria which impact upon security system definition at Navy shore-based facilities. The following nonexhaustive listing of directives are potentially applicable to the range of Navy sites involving NAVFAC design responsibilities:

1. U.S. Physical Security and Loss Prevention Manual, OPNAVINST 5530.14A (85)
2. Information Security Program Regulation, DOD 5200.1-R (August 82)
3. Physical Security Standards for Sensitive Compartmented Information Facilities, DIAM 50-3 (May 80, reprinted May 83)
4. Guidelines for Facility Design and Red/Black Installation, National COMSEC Information Memorandum (NACSIM) 5203, National Security Agency, (C) (June 82)
5. Department of the Navy Automatic Data Processing Security Program, OPNAVINST 5239.1A (April 85)
6. Cryptographic Security Policies and Procedures, CSP-1 (December 81)
7. Department of the Navy Information Security Program Regulation, OPNAVINST 5510.1G (April 84)
8. Department of the Navy Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E), OPNAVINST 5530.13 (December 81) (Change no. 1 dtd. 12/20/83)

9. Physical Security, NAVFAC Design Manual 13.01 (March 1983)
10. Intrusion Detection Systems (IDS), NAVFAC Guide Specification NFGS-16727
11. NAVFAC Guide Specifications as required for security lighting, cathodic protection, cabling, fence, and other security elements to be included in proposed system designs
12. Intrusion Detection Systems Handbook, SAND 76-0554, Information Systems Dept. 1730 Sandia Laboratories, Albuquerque, NM

1.3 How-To Use This Manual. This DM is intended to be used as a process-oriented guide for personnel responsible for the design and implementation of integrated electronic security systems at shore-based Navy installations. This DM should be used in conjunction with the structural guidance contained in DM-13.01 (Physical Security), other design manuals applicable to electrical systems, and various guide specifications appropriate to the proposed design. Specifically, NFGS-16727, "Intrusion Detection Systems," relates to required intrusion detection systems' elements.

1.3.1 Organization and Application of This Manual. Persons experienced in the design of integrated intrusion detection systems may wish to go directly to NFGS-16727 and use appropriate sections of this specification to develop the required design for the facility under review. Sections 2 and 3 of this DM permits those with limited experience in IDS applications with a general background on the range of options and a process for selecting the design solution appropriate to each site. Sections 4 through 8 provide guidance on various devices and subsystems which may be applicable to the site. Section 9 provides several generic sites with potential applications of devices; Section 10 sets forth a site survey format which design teams may find useful as a starting point for more comprehensive evaluations of IDS requirements. The basic process for using this and other design manuals is shown in Figure 1.

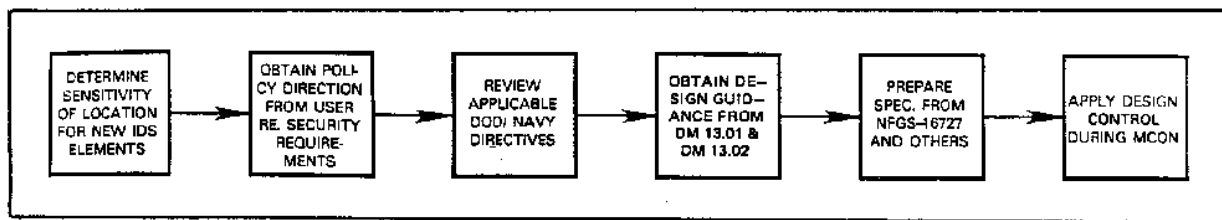


Figure 1
Relationship of DM-13.02 to MCON Implementation Process

Section 2: ELEMENTS OF INTRUSION DETECTION SYSTEMS

2.1 Introduction. This section introduces the total systems approach to security system design. The following paragraphs provide some basic information on those elements comprising subsystems which are complementary to electronic intrusion detection devices and underscore the principle that these IDS elements are but a part of a whole.

2.1.1 System Integration. The term system integration describes the critical process of completely incorporating and interfacing the various physical elements (barriers, security devices, etc.), personnel, and procedures into a site specific unified system which reduces and controls vulnerability. Importantly, it is the culmination of the security planning process described in OPNAVINST 5530.14 (U.S. Navy Physical Security Manual), in this and related NAVFAC design manuals, and in other Navy/DoD security directives.

2.2 Security Subsystems Overview. An integrated security system, through its various subsystems, discourages, detects, and defeats potential adversaries. The macro subsystems have the following functions in their relationship to the adversary:

- a) Physical resources to delay and deter the adversary;
- b) Equipment installed to detect and assess alarms caused by intrusion attempts and unauthorized activities;
- c) Personnel used for security system operations, management, and support;
- d) Procedures essential for system operation and effectiveness;
and
- e) Personnel equipment for security force support.

The remainder of this section summarizes several subsystems available to the user/designer relative to the system design task. It is not within the scope of this manual to discuss these options in detail, but instead to concentrate upon interior and simple exterior IDS systems. However, based upon the relative sensitivity of the site and the array of threats postulated against the security system, each of the subsystems depicted in Figure 2 should be considered as contributing to a final design solution.

2.3 Barrier/Delay Subsystem. The purpose of the barrier/delay subsystem is to channel personnel, vehicles, and materials through control points within a protected area and to discourage, deter, and delay unauthorized penetration attempts. The principles, techniques, and design criteria for several elements of this subsystem are extensively treated in NAVFAC DM-13.01, "Physical Security." The Naval Civil Engineering Laboratory (NCEL), Port Hueneme, California has developed a Penetration Resistance Rating

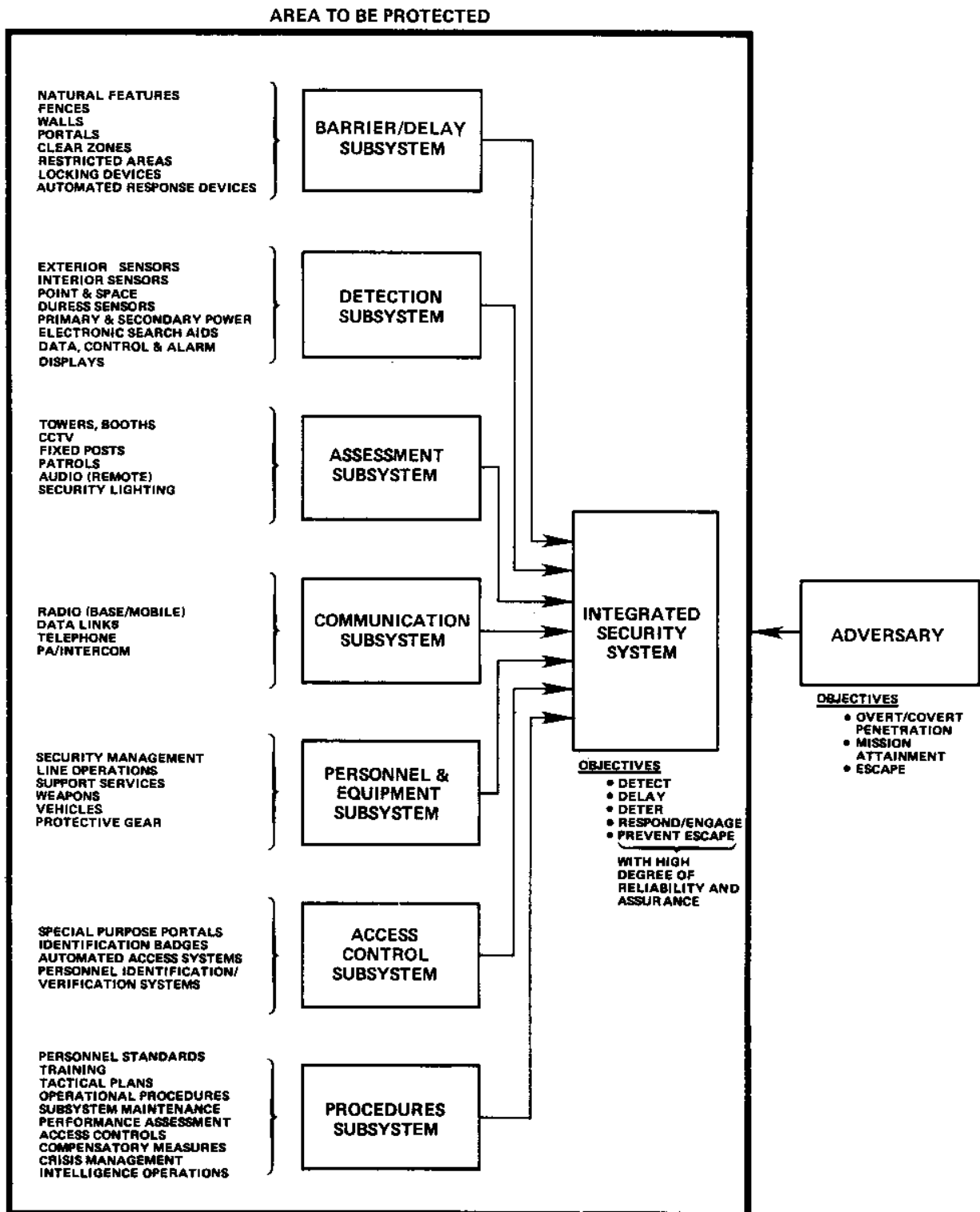


Figure 2
Security Subsystem Options

System (PRRS) to aid in the integration of construction materials and intrusion detection components. In very limited high security applications, the automated response devices noted in Figure 3 may also be considered required or appropriate. Present DoD policy specifies that these devices be nonlethal. Barrier/delay elements will be issues of concern in the planning of Restricted Area countermeasures (OPNAVINST 5530.13 Department of the Navy Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E) and OPNAVINST 5530.14) and various information security requirements (DIAM 50-3 Physical Security Standards for Sensitive Compartmented Information, OPNAVINST 5510.1G, etc.). With the increasing attention and use of electronic access control devices, the configuration of portals and the channeling of personnel through ingress and egress points is becoming more of a concern as well.

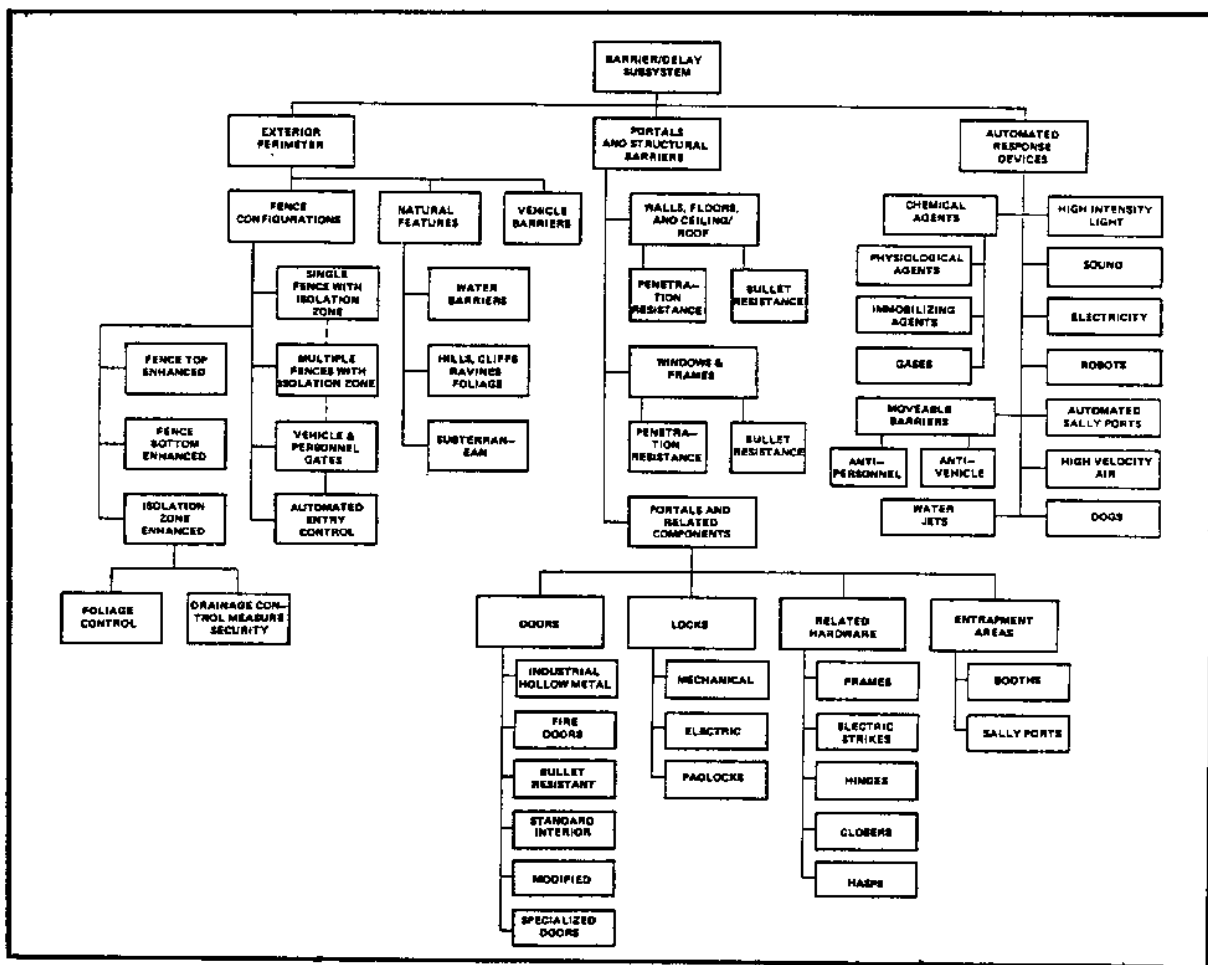


Figure 3
Barrier/Delay Subsystem

2.3.1 Barrier/Delay Subsystem Elements. The various elements which will typically be encountered in Navy facilities include, but are not limited to, the following:

a) Natural features such as bodies of water, ravines, hills, etc, which can both impede the adversary or provide cover to his covert penetration of the site. Foliage and other natural features can also impact the

13.02-5

performance of security subsystems and create vulnerabilities in system performance.

b) Clear zones to permit unimpeded surveillance and observation by security forces via electronic direct means. Clear zones are also used to create a friendly environment for exterior sensor systems.

c) Fences to delineate boundaries of restricted areas and form the outer perimeter of the security system to delay access to intruders. Fences also limit the environmentally generated causes of nuisance alarms on exterior sensor systems caused by animals, blowing debris, etc.

d) Walls and other structural components to prohibit and delay access and form an inner series of perimeters for specific assets.

e) Portals to control the flow of persons, materials, and vehicles into and exiting protected areas. Portals become the focal points for several elements in related security subsystems.

f) Hardened and special purpose structural materials to resist and delay hostile attack, provide protection to personnel located within, and protect against covert gathering of classified information.

g) Locking devices to restrict access to protected areas to specific groups or individuals.

h) Special purpose, limited application response mechanisms which can be remotely activated to deter and delay intruder penetration of highly sensitive areas.

2.4 Detection Subsystem. The detection subsystem provides electronic sensing and reporting of man, machine, and contraband items moving across, over, under, or through protected areas and perimeters or through control points. This subsystem increases control over specific points or spaces within a protected area by electronically sensing one or more types of phenomena and reporting outputs to the security response organization. See the potential inventory of detection subsystem elements in Figure 4.

2.4.1 Detection Subsystem Elements. Specific detection subsystem requirements will be in accordance with the needs and priorities of local activity commanders and applicable Navy and DoD directives. The principal exceptions to this are in sites possessing nuclear assets or conventional AA&E and those locations having extensive exterior perimeter sensor requirements. These fall within the purview of Naval Electronic Systems Command

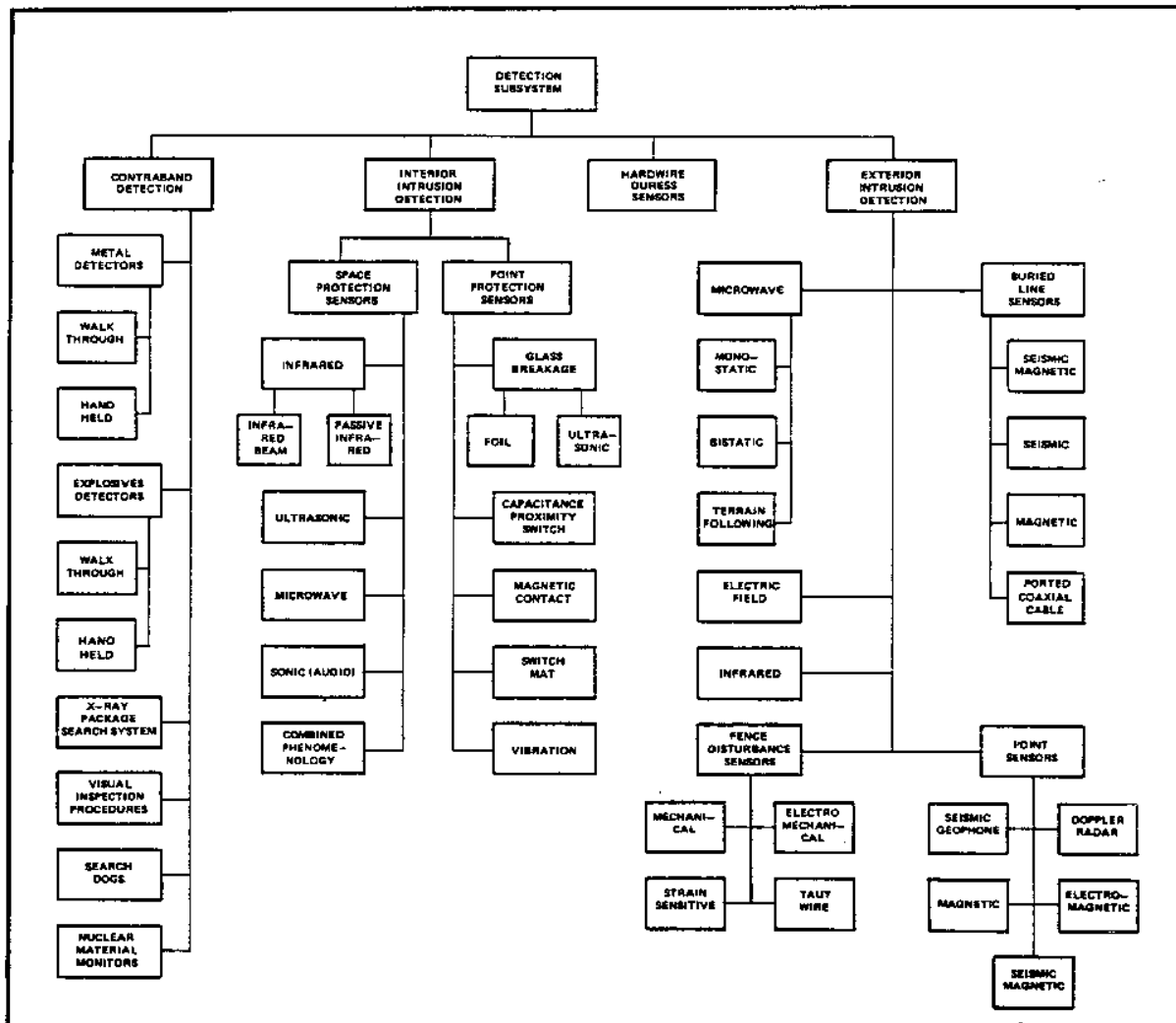


Figure 4
Detection Subsystem

(NAVELEXSYSCOM). Consistent with these limitations of NAVFAC responsibilities and within the scope of this manual, the contraband detection and more sophisticated exterior sensor elements noted herein are discussed only insofar as they may be Navy-wide considerations in particularly sensitive or critical sites.

2.4.1.1 Examples of Detection Subsystem Elements Include:

a) Exterior sensors deployed singularly or in overlapping configurations to maximize detection probability around protected area perimeters. These sensors may be attached to barriers (fences, gates, walls, etc.) or installed above or below ground. They use a variety of phenomena to sense intrusions and require careful analysis, specification, site engineering, and installation to ensure adequate performance. If security vulnerabilities can only be solved by the installation of exterior

sensors, the NAVFACENGCOM activity should contact the NAVELEXSYSCOM Remote Sensor Project (PDE-120R) for appropriate technical assistance.

13.02-7

b) Individual resource protection systems designed specifically to protect critical assets such as aircraft, tactical system individual elements, or other stand-alone special purpose resources.

c) Interior space and point protection sensors to remotely alarm upon entry to critical areas or access to critical items while minimizing the need for manned security posts.

d) Devices or nonelectronic means of detecting contraband prior to entry to protected areas.

e) Manually-actuated duress alarms to permit employees, security, or other key personnel to signal law enforcement or security control points in the event of a life-threatening event.

f) Data communications devices and media to ensure highly reliable and secure alarm signal transmission from sensor devices to the security control center. Alarm reporting, display, control and video assessment elements at this center provide the security/law enforcement organization with a system control network which facilitates effective command, control, and communications for timely response to verified threats to site security. Communication network elements are shown in Figure 5.

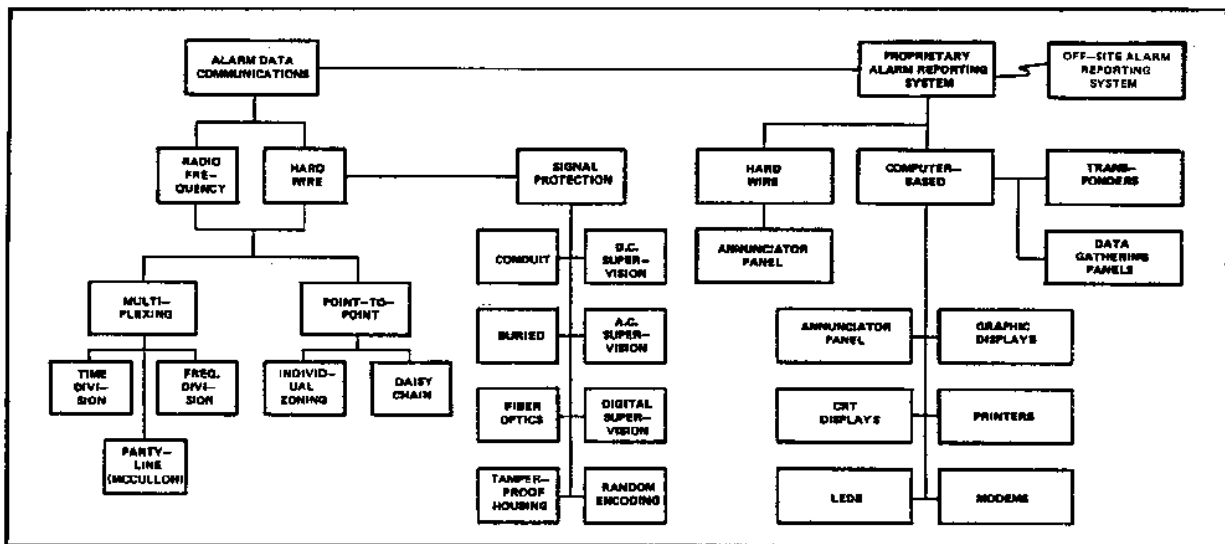


Figure 5
Detection Subsystem Communications & Control

g) Detection (and related electronic) subsystem support and performance elements to enhance total system operation and integrity. These elements are displayed in Figure 6.

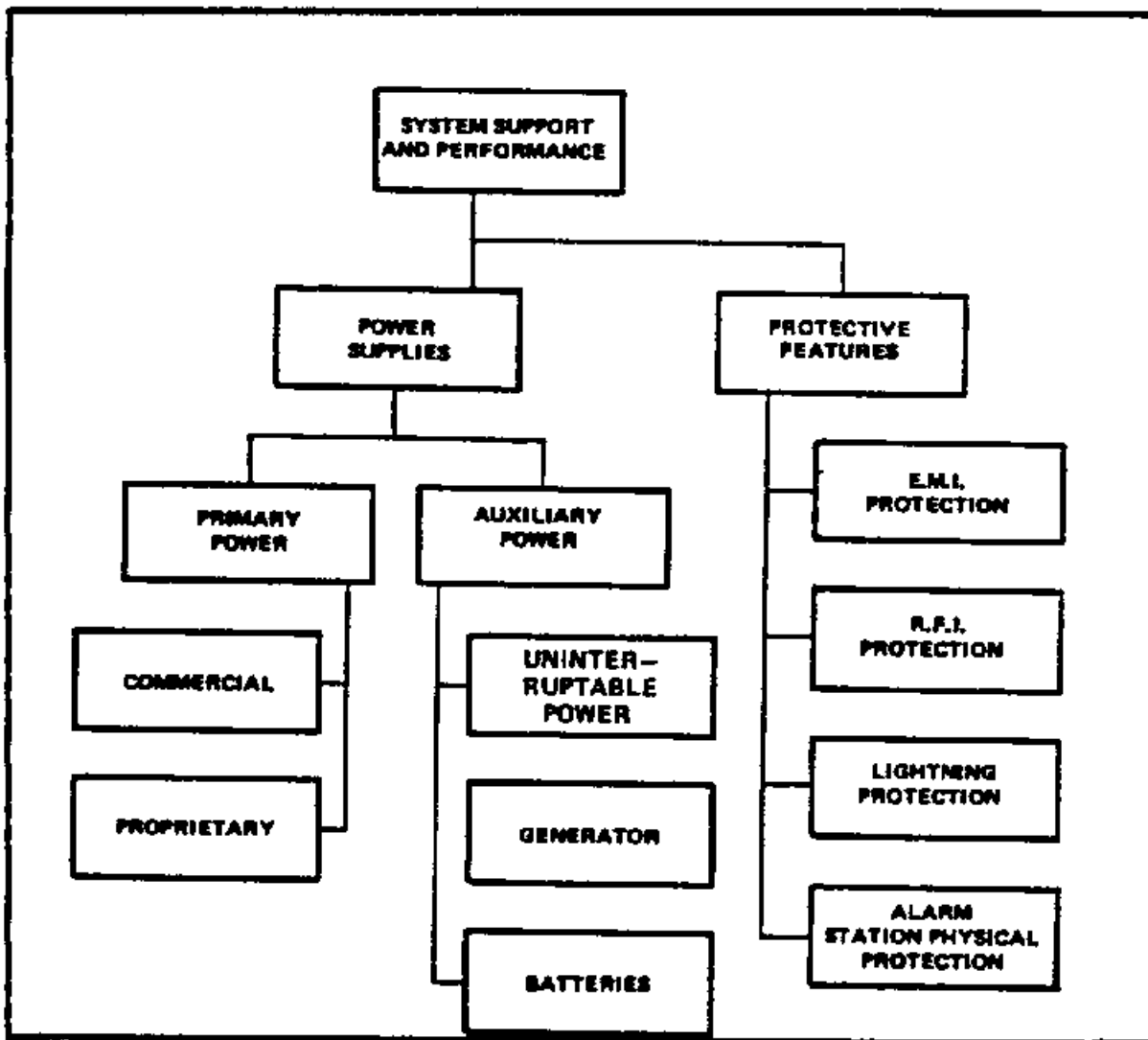


Figure 6
System Support and Performance Elements

2.5 Assessment Subsystem. The annunciation of remotely dispersed intrusion detection devices throughout large facility complexes creates a need for the response force to be aware of the validity, severity, and nature of the event that triggered the alarm. This requires the strategic placement of manned security posts, mobile patrols, or closed-circuit television (CCTV) throughout various protection zones. CCTV, particularly where these devices are installed to be activated in conjunction with a sensor in alarm status, significantly enhances the safety and response effectiveness of the security force and reduces the need for expensive and limited use of fixed security posts. Lighting is also an integral part of the assessment subsystem. These elements should be included in the overall security design to ensure CCTV camera performance and adequate surveillance

capabilities of the response force.

2.5.1 Assessment Subsystem Elements. In summary, assessment counter-measures that may be incorporated in total system designs may include those described briefly here and displayed in Figure 7.

a) Booths, towers, reception control desks, and other fixed security posts which provide for direct visual observation of critical points within a protected area.

b) Vehicle or foot patrols to provide for mobile surveillance of interior and exterior sectors of the protected area by the security force.

c) Closed-circuit television surveillance of critical access points and alarm assessment in conjunction with area-specific annunciation of intrusion detection sensors. CCTV may also be employed for area surveillance of high risk areas as a deterrent and as an activity recording element.

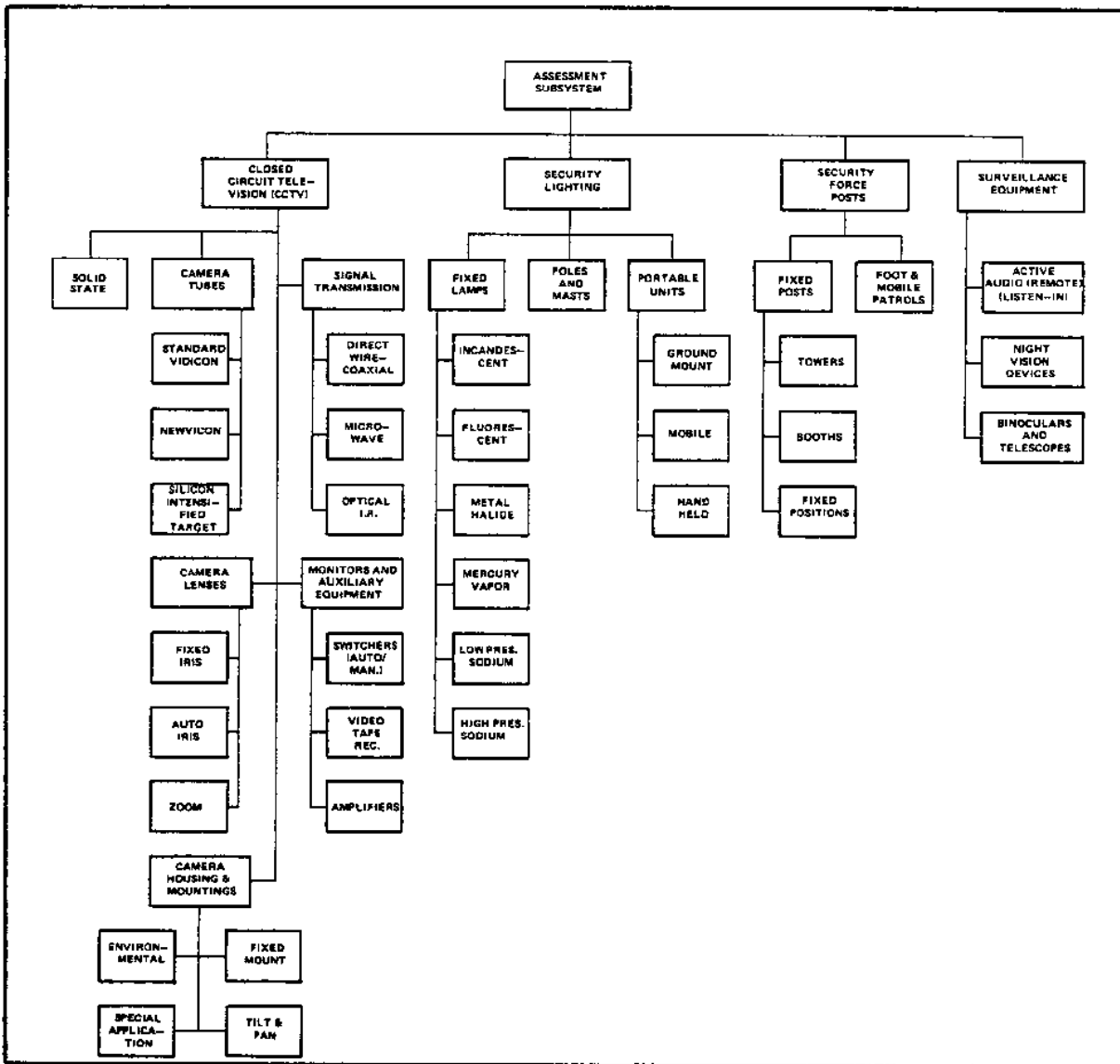


Figure 7
Assessment Subsystem Elements

d) Security lighting to enhance safety, security force surveillance, and video assessment capabilities.

e) Audio microphones as stand-alone devices or in conjunction with specific types of detection devices which provide audible signals. Other limited application devices include vision enhancing equipment used by the security force. These include sophisticated night vision devices and conventional binoculars and telescopes.

2.6 Access Control Subsystem. The access control subsystem complements the barrier and detection subsystems and provides automated electromechanical or procedures-oriented entry authorization/verification for personnel access to restricted areas. This subsystem controls and limits entry to spaces identified as sensitive, to specific individuals or classes of approved personnel, to vehicles, or to materials. Access authorization is based upon established access criteria and verification that the person seeking entrance is, in fact, electronically or procedurally approved. Minimum standards for ingress and egress control measures are established by OPNAVINST 5530.14 specifically for Restricted Areas (Exclusion, Limited and Controlled) and generally for all naval installations and activities. Depending upon the mission and sensitivity of the site, other more stringent or specific access control requirements may be dictated by Navy or DoD policy and the policies of the local activity commander. The various elements of the access control subsystem are shown in Figure 8.

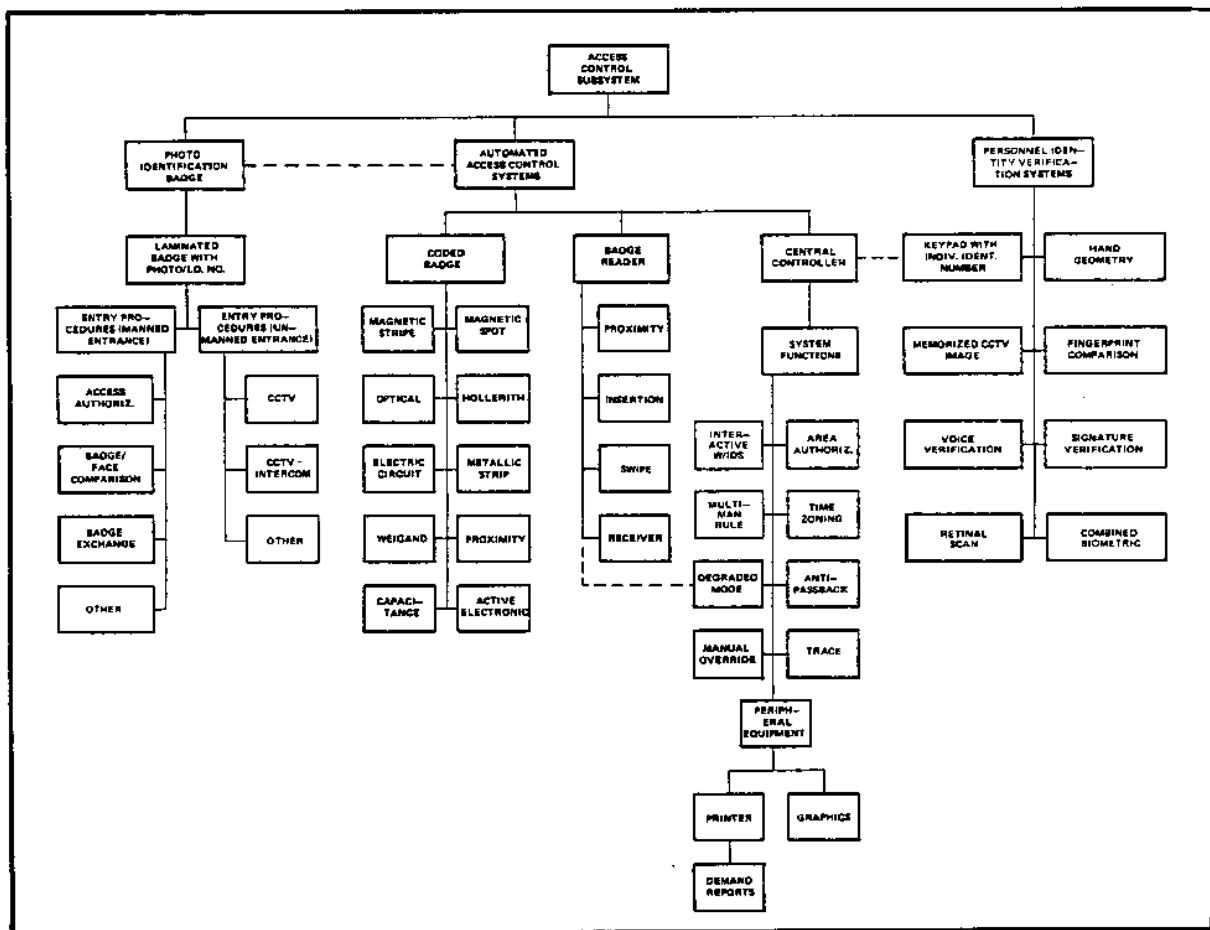


Figure 8
Access Control Subsystem Elements

2.6.1 Access Control Subsystem Elements. The two basic subsystem approaches to the control of personnel access to protected areas are:

2.6.1.1 Personnel/Procedures-Intensive Elements. These elements are primarily comprised of those approaches set forth in OPNAVINST 5530.14. They involve the use of approved systems with increasing levels of control as determined by security requirements which include:

- a) Military and dependent identification cards.
- b) Personal recognition by access control posts of those seeking entry to protected areas.
- c) Pass and badge systems implemented by activity, installation, or major commands which use identification card-based access controls. Within this category, specific protected areas may supplement this means of control with access list systems (logging procedures) for positive personnel identification, by badge exchange procedures, and/or via authorized escorts to control visitor access. These systems often use entry/egress control at primary entrance points to facility perimeters.

2.6.1.2 Machine-Intensive Elements. These elements electronically perform the entry authorization/verification process utilizing a variety of technologies and preestablished, mostly automated access criteria. These systems range from small applications providing control over a very few portals to large, distributed, computer-based networks which are capable of performing multiple security functions. The elements which may be configured with machine-intensive systems include:

- a) Microprocessor to large mainframe-sized central control units which incorporate various automated access criteria based upon area authorization, time zoning, multi-man access rules, anti-passback prohibitions, and other features. Where properly configured and programmed, these control units can also be used as the annunciation control for intrusion detection and assessment systems.

- b) Card-based entry control devices which electronically read preprogrammed data unique to each card and authorize or deny access attempts at specific portals. Cards may also serve as identification badges. Reader elements maybe employed on both entry and exit as stand-alone units or in conjunction with positive personnel identification devices.

- c) Positive personnel identification/verification elements are being used increasingly in high security applications where more than one (e.g., the card alone) access authorization criteria is required. These elements may include coded keypads, CCTV for facial confirmation or biometric readers to key upon the unique features of each authorized individual, such as hand geometry, speech, fingerprints, signature, etc. Barrier subsystems may be integrated into access control elements through the configuration of turnstiles, sally ports, and structural components to properly channel the

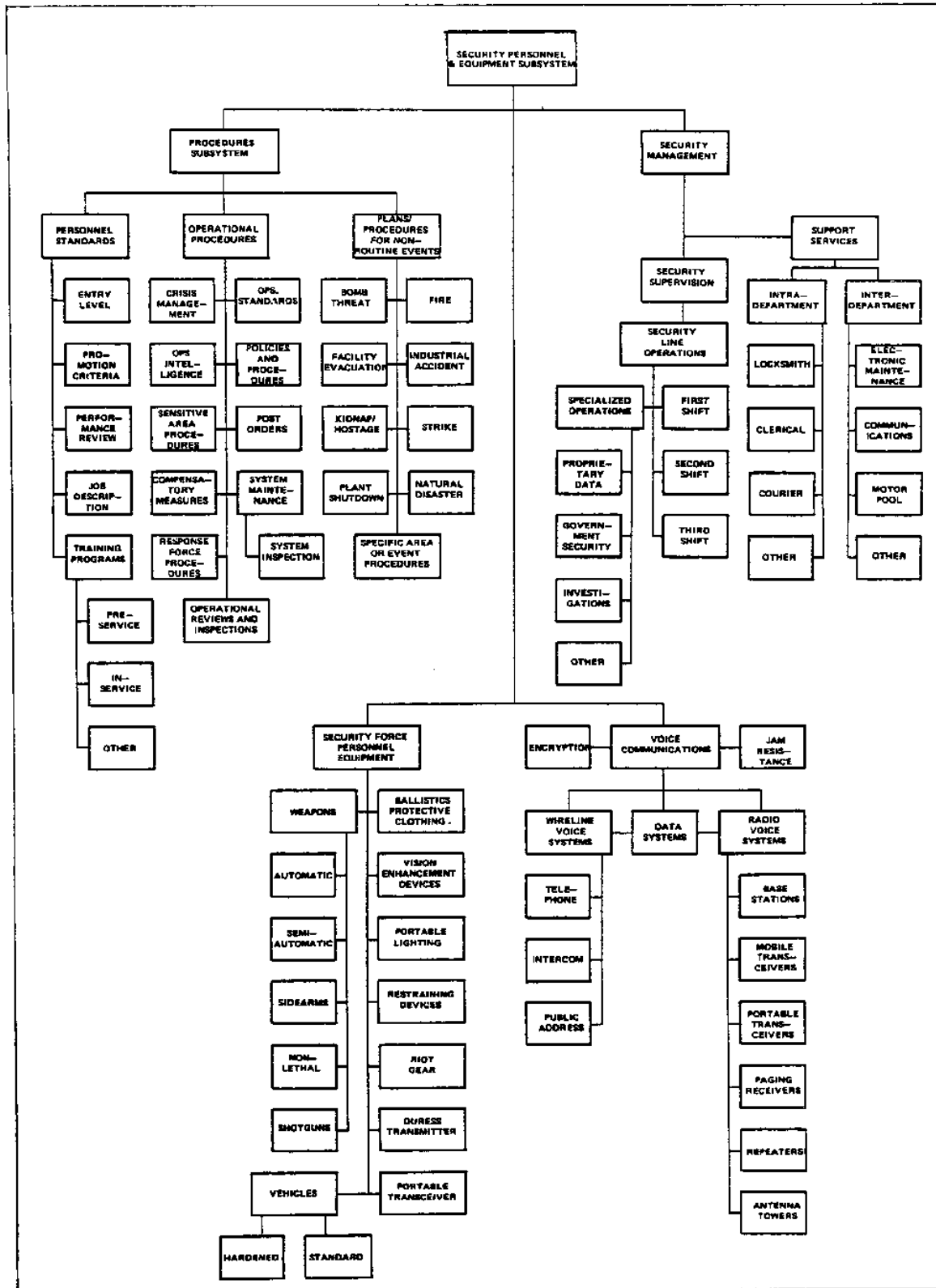
flow of people through controlled portals while facilitating throughput during high use periods.

2.7 Related Subsystems. The fully integrated security system must also incorporate elements from several other subsystems in addition to those briefly discussed above. These include voice communications, personnel and equipment and, most importantly, the procedures subsystem. While the elements included in these subsystems must be integrated by the end user, their requirements need to be considered in the security system design process throughout the various phases of project implementation. These subsystems are displayed in Figure 9.

2.7.1 Personnel and Equipment Subsystem. This subsystem provides the critical human interface of the total security system with the adversary to accomplish the ultimate objectives of deterrence, delay, detection, response/engagement, and the prevention of adversary escape. These total system objectives cannot possibly be achieved without the timely intervention of properly equipped and qualified operational personnel directed by competent and motivated supervisors. All of the subsystems discussed in this section are used, acted upon, or directed by the personnel subsystem.

2.7.2 Procedures Subsystem. The procedures subsystem is needed to completely organize the total security system and give policy direction to its implementation on a day-to-day basis. The elements include plans, manuals, standard operational procedures, and other guidance which are essential to system operation and integrity. The most reliable hardware installed in conjunction with the most effective barriers and related subsystems can fulfill their functions only when security personnel completely understand their functions and duties during both normal and emergency operations.

2.8. Summary. Clearly, hundreds of elements exist in the security system user/designer's inventory of choices. While many of these may only be found in the most secure sites possessing particularly sensitive assets, the need to integrate some components from each of the subsystems is common to all Navy activities where security is a concern.



Section 3: BASICS OF SECURITY SYSTEM DESIGN

3.1 Introduction. In a very real sense, the security system design process is never-ending. The decision to implement a security program, regardless of the subsystems or elements employed, is made out of the realization that there is a threat which must be controlled. The process must continue because of the dynamic and ever-changing nature of threats confronting U.S. military facilities. The design process, therefore, first considers the range of events potentially confronting the site or asset to be protected, then considers what the consequences of loss or compromise would be and what it might take to deter and prevent such events from occurring. Once installed and operational, the user continues to focus on how the array of threats is changing and how these changes might impact the countermeasures now in place. Is the system capable of meeting these new circumstances? This section focuses on a process that has proven to be both comprehensive and easily adaptable to any design whether large or small. Depending upon the complexity of the security mission, it can be extremely short in duration or consume many man-months of effort. In every case, each of the four basic phases should be followed sequentially as required by the unique circumstances at each site.

3.2 Facility Categorization. Any comprehensive attempt to neatly categorize all types of naval facilities into one listing that fits every application would clearly fail. More importantly, it would overlook two critical factors: first, each site is unique based upon a variety of local circumstances and, second, the local activity may have justifiable concerns for increased levels of security. The following discussion, therefore, is necessarily general in scope, and each requirement of security countermeasures must be evaluated on a case-by-case basis as determined by "higher level" and local policy.

3.2.1 Factors Influencing System Design Criteria. There are several factors which clearly influence the security system designer as he approaches the requirements of each site. These include the following:

- a) The specific requirements of DoD and Navy directives which prescribe security countermeasures for various types of USN facilities, activities, and assets. These directives are complemented by the specific requirements for security laid down by activity commanders at shore-based installations. While these countermeasures may be modified by waivers and exceptions, availability of funds, or other resources or local circumstances, they comprise a baseline from which to evaluate basic security system capability requirements and other design criteria.

- b) The sensitivity (criticality) of the asset(s) to be protected. This is a basic element of impact or consequences analysis and focuses upon the "what if" questions to a variety of event scenarios. The ultimate

resolution of these issues tends to conclude with assessments of loss or reduction of mission capabilities at the highest levels of concern and scale downward to lesser consequences based upon the criticality of the assets to be protected.

c) Based upon the critical nature of the activity and the relative consequences of various events posed against it, the more sensitive or critical the asset, the more dynamic and potentially sophisticated the threat(s) against it. The corresponding security system design objective is to build sufficient countermeasures to adequately control this range of threats.

d) The fourth factor influencing the design process is the inherent capability of the site in terms of protection. The various gaps in its protection capabilities against the identified threat(s) equal its vulnerability to attack. The ultimate objective of the design process is to minimize and control each of these vulnerabilities.

e) Other factors influencing the design process are the ever-present realities of cost, time, local resources and capabilities, operational requirements of the activity, and a range of additional constraints. These can be the ultimate determinants of the final design solution and must not be overlooked by the process.

3.2.2 Facility Sensitivity/Criticality. Based upon activity criticality, certain generic, top level categorizations of the range of USN shore-based installations may be made as indicated in Table 1. These are subject to increased or decreased emphasis based upon the dictates of local or major command policy and applicable facility security directives.

Table 1
Facility Categorization by Criticality

Category A [*]	Category B	Category C	Category D
<ul style="list-style-type: none"> o Nuclear ordnance o Other nuclear o Conventional AA&E o Tactical/Strategic mission essential USN resources outside of CONUS 	<ul style="list-style-type: none"> o Sensitive compartmented information (SCI) facilities o Tactical/Strategic mission essential USN resources in CONUS o Exclusion areas IAW OPNAVINST 5530.14 o Facilities committed to support mission essential resources <ul style="list-style-type: none"> o POL o Power o Comm. o Etc. o Security control centers 	<ul style="list-style-type: none"> o Limited and Controlled areas IAW OPNAVINST 5530.14 o Controlled industrial areas in shipyards o Areas containing high value inventory in break bulk o Areas containing sensitive inventory IAW OPNAVINST 5530.14 o Funds/negotiable instruments storage o Offices containing classified information IAW OPNAVINST 5510.1G 	<ul style="list-style-type: none"> o Command quarters o Offices, buildings designated o General support and training facilities o Naval exchange commissaries etc. o Motor pool o Piers & wharves o Key storage o Nontactical & power centers o Other special physical spaces
<p>[*] Responsibility of COMNAVELEX</p>			

3.2.3 Threat and Consequences of Events. Facility sensitivity/ criticality concerns highlight the potential array of threats posed against the asset(s) and upon the consequences of one or more of these threats occurring at the site. Thus, a Category B facility seen in Table 1, when confronted with the four generic levels of threat indicated in Table 2, yields an equally broad range of potential consequences and required security system capabilities. The planning process must initially focus upon the range of assets to be protected by the proposed system and then carefully consider what kinds of threat categories might try to compromise security to carry out their mission of sabotage, theft, etc. Actual event data at the site or elsewhere coupled with intelligence from Naval Investigative Service (NIS) or other investigative agencies is particularly important during these early stages of system planning. The user activity needs to define the upper range of threat they want the security system to deter and detect. This usually results in tradeoff analysis (cost/benefit considerations) where the consequences of loss or compromise are not directly tied to Navy mission capabilities of the user activity. The expenditure, therefore, of \$10,000 to secure against the one-time loss of \$5000 of consumable inventory is questionable. Yet, the expenditure of \$10,000 to secure the fueling capabilities of tactical aircraft, even in the face of no prior events, may have clear justification.

3.2.3.1 Categories of Threat. Table 2 sets forth four broad and generic types of threat for the user activity to specify as a basis for the security system design. In several instances, activity commanders or other elements of the Navy or DoD may specify in detail a design basis threat and required system performance capabilities. As in the first phase of the process discussion (subparagraph 5 of this section), the specification of a design basis threat is essential to determining the vulnerability of the asset. The security system is then designed with the objective of controlling and minimizing these vulnerabilities.

3.3 Specific Requirements of DoD and Navy Directives. Among the several threat and site sensitivity/criticality factors that must be considered by the system design process, the specific policy directives of the Navy and DoD also place design parameters on alternative solutions. It is the responsibility of the system designer to confirm the applicability of appropriate directives issued by local activities or higher authority. In many applications, multiple sources may be involved and, in specific types of facilities, certification or other forms of approval will be required. The listing of directives in Table 3 represents a nonexhaustive inventory of sources of concern to NAVFAC shore-based installations.

3.4 Basic System Design Considerations. Several basic considerations should guide the system designer as he proceeds to lay out the proposed intrusion detection system. It has been proven time and again that failure to fully consider these basic concerns will invariably lead to poor system performance, excessive cost, and/or user dissatisfaction.

3.4.1 Know the Environment. The best equipment, perfectly installed and maintained, can completely fail in its protection mission if the design has failed to account adequately for the physical and operational environment in which it must function effectively. The result is a system that becomes an annoyance and leads to shutdown and costly retrofit.

Table 2
Range of Threats and Consequences

Threat Level	Nature of Threat	Motivation	Methods	Potential Consequences	Required Security System Capabilities
Maximum	<p>Knowledgeable skilled & well-equipped intruders using sophisticated penetration aids that can be carried with them.</p> <p>Outsiders in highly organized group working alone or in collusion with knowledgeable insider.</p>	<ul style="list-style-type: none"> Assassination Extortion Sabotage Espionage Destruction of vital equip. or military asset(s) 	<ul style="list-style-type: none"> Forcible entry Covert entry in collusion with insider associate(s) Extortion of insider(s) Gain access to extort 	<ul style="list-style-type: none"> Destruction of vital assets Injury/loss of life Reduction of tactical or strategic readiness Compromise of data Propaganda 	<p>Immediate detection with adequate time for response prior to adversary achieving objective. Complete penetration denial and neutralization or elimination of adversary. Prevent escape.</p>
Advanced	<p>Knowledgeable or semi-skilled intruder without penetration aids.</p> <p>Outsider working alone or in collusion with an authorized insider.</p>	<ul style="list-style-type: none"> Sabotage Espionage Theft Propaganda Deranged or fanatical 	<ul style="list-style-type: none"> Forcible entry Bypass access controls Stay-behind Plant covert device(s) Explosive device, arson, etc. 	<ul style="list-style-type: none"> Intentional damage to vital equipment Compromise data Personal injury Loss of asset(s) Reduction of mission capability 	<p>Early detection & response. Complete penetration denial to access to asset(s) and prevention of sabotage, theft or accomplishment of adversary objective. Capture of intruder.</p>
Intermediate	<p>Intruder familiar with security system but ignorant of installation characteristics and total system capabilities. Includes stand-off threat from surveillance.</p> <p>Outsiders alone or in small group. Insider working alone.</p>	<ul style="list-style-type: none"> Espionage Sabotage Theft Disgruntled employee Activist Carry out threat for propaganda 	<ul style="list-style-type: none"> Attempt forced entry or covert access to assets Stealth Insider without access authorized to restricted area Stay-behind 	<ul style="list-style-type: none"> Intentional damage to vital equipment Compromise or loss of data or asset(s) Propaganda/media attention to lax security Reduction of mission capability 	<p>Same as for Advanced. Denial of access and surveillance opportunity. Response within sufficient time to prevent escape and minimize impact.</p>
Basic	<p>Casual intruders, demonstrators, petty thieves, pilferers, etc.</p> <p>Outsiders alone or in groups and insiders working alone or in association with other insiders.</p>	<ul style="list-style-type: none"> Theft Vandalism Curiosity Perceived right Political activism Drug or alcohol dependent Disgruntled employees Labor unrest 	<ul style="list-style-type: none"> Malicious damage or destruction of Gov't property Forcible entry Covert theft Unescorted walk-in Arson Disruption of operations and capabilities Staged media events 	<ul style="list-style-type: none"> Breach of security Injury to intruder or personnel Propaganda and political/public relations hostility Loss or compromise of asset(s) Costly repairs and maintenance 	<p>Detection and deterrence or apprehension of intruder. Prevention of intentional or accidental damage, vandalism, theft or other impacts to mission capabilities.</p>

Table 3
DoD and Navy Physical Security Directives

SOURCE DIRECTIVE	INTRUSION DETECTION SYSTEMS	REMOTE ALARM ASSESSMENT SYSTEMS	ALARM DISPLAY AND DATA COMMUNICATIONS	CARD ACCESS DEVICES
1. OPNAVINST 5530.14	Chapter 8 inclusive. Appendix VII INTERIOR SYSTEMS: DoD standards to be followed (J-SHDS) or commercial equip. approved by CNO (OP 008). EXTERIOR SYSTEMS: Approved of design and equip. configuration by NCO (OP 008). INSTALLATION: Required by Public Works, NAVELEX or U.L. approved contract installer. Contracted installation to utilize security procedures calculated to protect details of protective measures from noncleared sources. Installer/maintenance firm/personnel to possess DoD clearances to specified levels. MAINTENANCE: Required for reliability. Tests to be performed minimum monthly and test results to be recorded with false alarm and other device malfunction data. TAMPER: All IDS equip. which can be opened to be fitted with anti-tamper device.	Par. 1105. General description of utility of CCTV as a complement to an IDS and as an aid to reduce dependence upon manpower at fixed security posts. Specific requirement for CCTV maintenance contracts in terms of component replacement policy.	Display units to be proprietary except where no Govt. response available. Local police or contract central station coverage for these latter cases. Proprietary systems to be monitored around the clock and provide both audible and specific visual alarm for each protected area. Control units, sensors and related equip. to be within the protected area. Alarm data transmission lines to be high security supervision techniques. Back-up power required for the IDS.	Chapter 5 establishes basic standards re Personal ID system. Electronic card access not required, but if utilized, card credential must meet Par. 0504 requirements.
2. OPNAVINST 5530.13	Contains Navy policy re conventional AABE with cognizant design/implementation responsibility assigned to NAVELEX.			
3. OPNAVINST 5510.1G	Chapter 11 contains guidance re physical security of classified material. Table A (Table of Numerical Equivalents) provides numerical values to specific countermeasures which includes protective alarm systems.			Card-based access controls are compatible with access requirements of storage areas when properly configured.
4. OPNAVINST 5430.48A (INCORPORATED INTO 5510.1G ABOVE)	Chapter 11, Par. 1115-1125, covers security alarm systems by type, application, installation requirements, etc. Essentially covers identical content of OPNAVINST 5530.14, Appendix VII re J-SHDS equipment (and DIAM 50-3, in part. 5430.48A applies primarily to the security of classified information.			General access control referenced as a primary element of information security.
5. DIAM 50-3	Chapter 3 applies to IDS installation requirements in Sensitive Compartmented Information (SCI) Facilities. The Defense Intelligence Agency (OS-2) should be contacted for specific guidance and approval on IDS component selection and application requirements for each site under their cognizant review. Chapter 2 categorizes generic sites by type and offers alarm systems as required or optional.	CCTV often employed for alarm assessment and visual access verification/surveillance. However, 50-3 does not specifically address these components.	Particular attention to the design of IDS data communications network required to preclude TEMPEST problems and ensure line date and physical security.	Card-based electronic access controls are compatible with access requirements to these types of facilities. However, the DIA criteria limit the number of approved sources.
6. CSP-1	Chapter 2 contains minimum safeguards matrix based upon site status. Alarm systems required on access points in sites not continuously manned. Alarm devices to meet GSA-PSS Spec. W-5-00450A or agency standards. Focus of protection is upon access points and storage vaults or containers.			Access requirements to communication areas can be met through card-based systems. However, design criteria must meet standards in Chapter 6.
7. NACSIM 5203	Incorporates provisions for specific installation standards.		Provides definitive guidance re RED/BLACK engineering requirements.	Provides access control guidance.
8. OPNAVINST 5239.1A	Chapter 3 and Appendix F establish guidance for ADP facilities referencing OPNAVINST 5530.14. Intrusion alarms cited as having high countermeasure confidence to access vulnerabilities.	Continual surveillance of the controlled area required. CCTV of interior/exterior a stated option.		Installation of an access control system at critical entry points and to specific ADP areas/devices.
9. NAVSEAINST C9210.22A	Confidential requirements for Security and Safety of Nuclear Reactor Plants, Fuel and Components Containing Plutonium or Enriched Uranium.	Applicable requirements.	Applicable requirements.	Applicable requirements potentially extending to card-based systems.
10. OPNAVINST 5530.15	Marine Corps Physical Security directive. IDS permitted at perimeters for early warning.	CCTV may be utilized in conjunction with IDS on boundaries and as a complementary measure at entry control points.		Process control at perimeters and critical areas within requires access control measures.

3.4.1.1 Physical. Electronic intrusion detection systems are designed to sense and report on stimuli in their areas of application. Failure to properly determine the environmental extremes in areas where various subsystems will be installed may lead to increased sensitivity and nuisance alarms or degraded performance and no alarm, excessive maintenance, and result in loss of user confidence. Temperature extremes, environmentally generated vibration, wind, fog, humidity, conducted and radiated electromagnetic interference, transient light sources, and lack of consistent power availability are some of the common causes of component performance problems. Adequate survey techniques and data analysis of the physical environment, over time, can substantially predict these extremes and factor them into the system design.

3.4.1.2 Operational. It is essential that how the facility works at all hours, under varying conditions and what the user activity requires for efficient operation, be factored into the system design.

3.4.2 Provide for Protection-in-Depth. Also known as security-in-depth or defense-in-depth, this concept is concerned with erecting and integrating physical and electronic countermeasures in concentric rings around the protected asset. The objective is to build time delays into the intruder's access to the asset and make it progressively difficult for him to reach his target undetected and escape. Placement of electronic detection and assessment hardware becomes critical to maximize the potential that he must pass through a detection pattern to carry out his mission. Protection in-depth is also concerned with providing assurances that failure of one element or component will not detract from the total capability of the system or any one critical area of protection. NAVFAC DM-13.01, Physical Security, discusses the role of physical barriers in protection-in-depth and time delay in great detail. Moreover, the Restricted Area requirements of OPNAVINST 5530.14 (para. 0306) reflect this concept in Navy security practice.

3.4.3 Provide for High Probability of Detection and Low Nuisance Alarm Rates. The system design process constantly strives to make the probability of detecting an intruder 100 percent and the potential for nuisance alarms zero percent. Both objectives are the ideal.

3.4.3.1 Probability of Detection (P_{rd}). The probability of an individual sensor detecting an intruder is calculated by dividing the number of attempts into the number of successful detections. Most commercially available sensors indicate a P_{rd} of 0.95. This has been based, however, upon tests of actual intrusions into the sensor field in a laboratory environment. Given the environmental impacts potentially available in the real world and the presence of a knowledgeable and determined intruder, P_{rd} needs to be evaluated as a system performance goal rather than as a measure of individual sensor performance. Thus, the location of the equipment to maximize detection, the potential use of multiple sensor arrays (redundancy), or different types operating on different stimuli (diversity) should be considered, particularly in higher security applications. These techniques are consistent with the protection-in-depth concept discussed above.

3.4.3.2 Nuisance Alarm Rate (NAR). Sensor subsystems should be designed and installed to generate the absolute minimum number of nuisance and false alarms per unit of time. False alarms are differentiated from nuisance alarms in that the former are caused by nonintrusion phenomena inherent to the system, such as a malfunction, while the latter are valid alarms generated by phenomena not within desired detection parameters. These include animals, wind, etc. Nuisance and false alarms are terms often mistakenly used interchangeably. Because nuisance alarms cannot be completely controlled in the typical installation, there is a growing technique of assessing alarm annunciations through closed-circuit television cameras covering the sensor field. This permits automatic assessment of a sensor zone on alarm and minimizes the need to deploy response forces if nuisance generated. Carefully designed sensor subsystems, even in the most hostile environments, can substantially minimize nuisance and false alarms to acceptable limits.

3.4.4 Design for Cost-Effectiveness. The requirement to maximize system detection probability and protection-in-depth does not mandate the saturation of protected areas with sensors, cameras, or other devices. Equally, once a decision has been made that the criticality versus threat circumstances require protection, "doing it cheaply" is just as inefficient and ineffective. Cost-effectively, one can utilize the appropriate mix of barrier, electronic, and procedural options keyed to the unique requirements of the site. Recent developments, as well as those now in research and development, are bringing the cost of electronic systems down in both equipment and installation. A comprehensive application of the design process will have the most immediate impact in both short term and life cycle costs of security systems.

3.4.5 Flexibility and Expansion. One of the most cost-effective measures to be taken is to build the security system for flexibility and future enhancement. It ordinarily follows that once properly installed and operational, the in-place system is periodically expanded to accommodate new alarm points, increased electronic access controls, expanded CCTV coverage, etc. Most modern alarm and video control systems are modularly expandable and permit future growth both on- and off-site. Designs should anticipate such expansion and not limit control elements, conduit, and other system components to the specific requirements of the immediate installation.

3.4.6 Build the Detection Subsystem for Point-for-Point Annunciation. Unless specified, contract installers may often daisy chain alarm devices to simplify the job and reduce their cost. This results in the annunciation of any number of devices at the reporting unit without giving the operator the benefit of knowing which device in the area is causing the alarm. Each alarm point should be wired separately back to the control unit on a dedicated zone for reporting to the control console. This technique also substantially eases troubleshooting by maintenance personnel and reduces downtime, repair time, and cost.

3.4.7 Build the System for Ease of Operation and Maintenance. Keep the system as simple as possible and carefully consider the interface of man and machine throughout its control function applications. In particular, at the

alarm control and monitoring location, ensure that the operator is not over-loaded with supervisory functions for the electronic elements. More than likely, he will have several ancillary duties. Limits have been established on the effectiveness of this critical function.

3.4.8 Provide for Critical Area Sensor Zones to be Tied Into CCTV Assessment. The adequacy of security force response depends upon the ability of the command and control function to reliably assess the nature of the alarm and to communicate in near real time the circumstances in the area. The installation of localized CCTV cameras tied into the sensor annunciation control network permits the operator to view immediately the alarming sector, verify the threat as real, and communicate relevant information to response forces. This is also useful during periods when nuisance alarms are being generated by environmental stimuli and as a check on maintenance in these sensitive sectors.

3.4.9 Integrate Security Subsystems for Total Protection. As discussed in Section 2 of this manual, the truly effective security system totally integrates barriers, equipment, people, and procedures into a functional whole. The system designer must identify the subsystem elements required for the unique protection needs of each definable area of the site and then build a total system to control each vulnerability. Too much reliance on electronics or any other subsystem will invariably overlook the dynamics of threat or other constraints on system performance.

3.5 Security System Design Process. It is imperative that the design process proceed through a comprehensive requirements analysis and preliminary design phase, despite how elementary the proposed application may be.

3.5.1 NAVFAC Responsibility for Security Requirements Analysis. This design manual does not suggest or recommend that NAVFAC, its contracted A&E firms, or system installation contractors be responsible for the gathering of intelligence and other information essential to the security requirements analysis. HIS, Federal, state, and local investigative agencies, as well as specific elements of DoD and Navy activities, have clear responsibilities in these areas. However, the integration of this information (at appropriate classification levels) into the NAVFAC-directed design is clearly essential to the MCON-related security system implementation process.

3.5.2 Consistency of the Security System and MCON Design Process. Generally, the MCON process is divided into four phases of varying duration and involves several deliverables: preliminary investigations and the preliminary design phase (concept study) leading to the 35 percent design, and the 100 percent design completion phase. Then the project is bid for construction/installation, checkout, and turnover. Below, the system implementation cycle is described in four phases from inception through turnover, phases 1 and 2 comprising up through the MCON 35 percent design; phase 3 leading to the 100 percent design and preparation for installation

(construction) contract; and phase 4 encompassing installation, test, acceptance, and turnover of the security system.

3.5.3 Phase 1 - Requirements Definition. The primary objective of the critical first phase of the process is the determination of vulnerability. As indicated earlier, a security system is only as effective as its ability to control and reduce vulnerability. The process commences, therefore, with a thorough analysis of the physical and operational environment in which the system must operate and the array of threats postulated against it. This is graphically displayed in Figure 10.

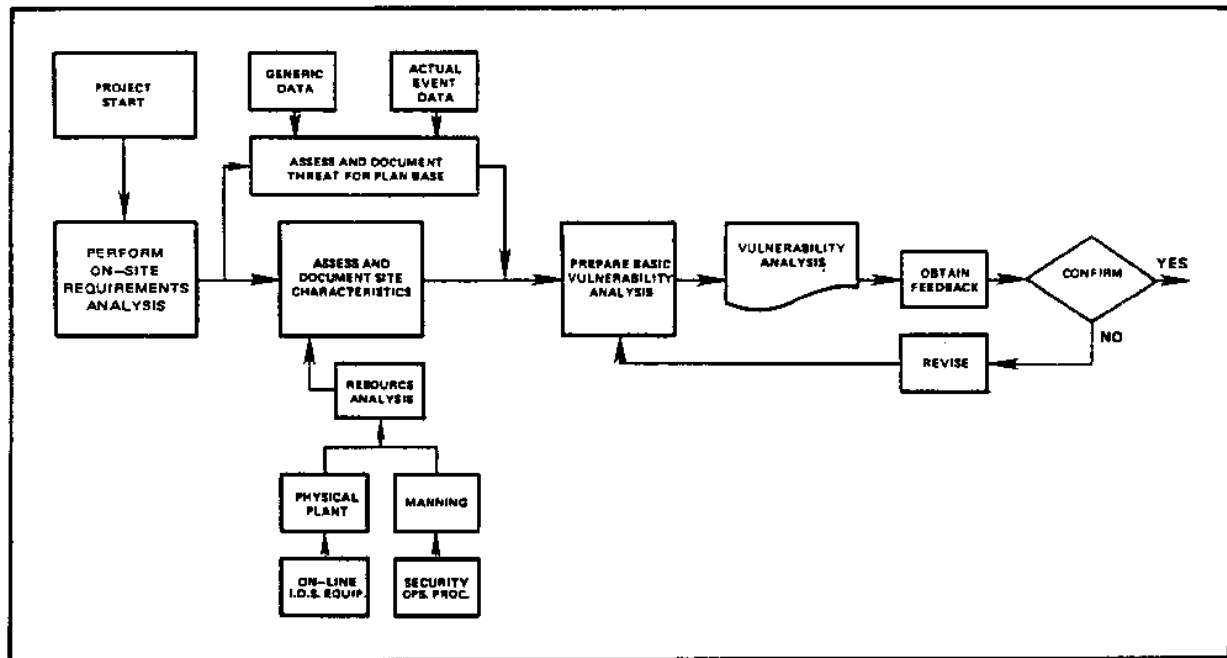


Figure 10
Phase 1 - Requirements Definition

3.5.3.1 Perform On-Site Requirements Analysis. The principal inputs to these first steps are resource and threat documentation. The site survey guide provided in Section 10 of this manual should be used as primary input into this phase of the design process.

3.5.3.1.1 Resource Analysis. Resource analysis provides a baseline of in-place or projected subsystem elements which contribute to the eventual design. The physical plant, for example, has walls, barriers, terrain, etc., with inherent delay capabilities. Various operational procedures are in place providing for management controls over identified assets. Each of these and other elements must be identified in order to determine their protective capabilities. This analysis is particularly important in retrofit applications. Cost/benefit/effectiveness alternatives are of critical

importance to management; more costly construction and installation options can often be rejected in favor of enhanced procedural controls or staffing. Alternatively, the continuing cost of manpower can be offset through correctly designed electronic subsystems. In the performance of the resource analysis, an in-depth assessment of the physical environment also needs to be completed. The presence of environmental attributes such as seismic activity (both man-made or natural), radio frequency and electromagnetic interference, weather conditions (rain, snow, fog, etc.), physical condition of barriers, lighting, heating, ventilating, and air-conditioning (HVAC), and other internal stimuli will contribute to later potential consideration of electronic sensor siting. Failure to fully evaluate these and related factors may completely negate the validity of successive subsystem recommendations.

3.5.3.1.2 Threat Analysis. The analysis and resulting specification of a design basis threat analysis is the responsibility of the Activity and appropriate investigating elements such as NIS. Most importantly, organizations must establish who the system is to deter, delay, and detect and how they may be expected to attack the protected area. Without this basic information, the remainder of the system design process may be directed toward overdesigning or underdeveloping a solution that is inappropriate to the real threat. Table 2 may be used as a generic guide in developing a site-specific design basis threat for protected assets.

3.5.3.1.3 Preparation of Vulnerability Analysis. Initial steps in the process have generated information on risk (exposure to hazard or loss) and threat (the source of the risk). This information must now be used to develop the focal point of the security system design: vulnerability analysis. Vulnerability may be defined as the relative accessibility of the area or item to be protected to specific risks or threats. As such, successive system design tasks will first determine the range of potential countermeasures which may be employed to remove or control these vulnerabilities and eventually lead to a site-specific set of solutions. The vulnerability analysis breaks out each asset, and given the adversary characteristics established in the design basis threat documentation, proceeds to a determination of the site capabilities to deter, delay, detect, and respond to carrying out the postulated adversary sequence. This is displayed conceptually in Figure 11. The vulnerability analysis asks the question, "What physical and procedural countermeasures must be defeated by the inside/outside adversary to successfully penetrate the protected area, carry out the mission, and effectuate an escape?" Several potential resources may exist to deter, detect, or delay entry at successive points. The outsider, working alone or with other outsiders, is confronted with the full range of subsystems incorporated in the security system. The insider may possess the ability to bypass one or more of the subsystem elements. Insider/outside collusion threats require the full consideration of redundancy, diversity, and the resulting defense-in-depth essential to security system effectiveness. A prioritized matrix of consequences will focus both the user and the system designer on specific vulnerabilities and provide a foundation for later cost-benefit considerations. The resulting analysis should be a focal point for discussion with the user, both to sensitize him to issues which will require future management support as well as to obtain consensus for direction in the early phases.

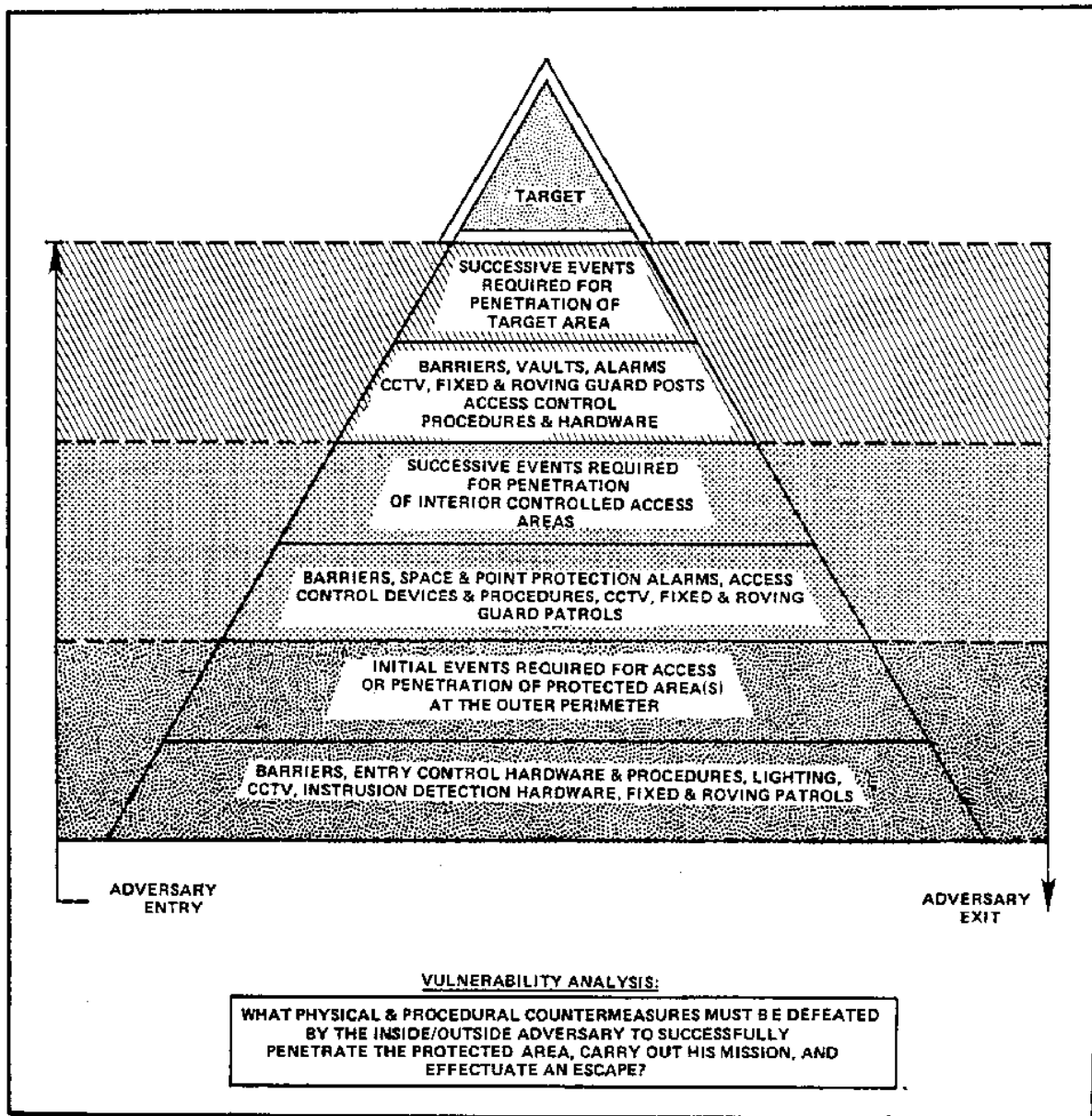


Figure 11
Vulnerability Analysis Process

3.5.4 Phase 2 - Development of Preliminary System Design. This second phase builds upon the essential input data generated in Phase 1, making the process now capable of developing candidate solutions for location and asset-specific vulnerabilities. The steps involved in this phase are shown in Figure 12.

3.5.4.1 Development of Security Upgrade Plan. The overall system concept is set forth in the upgrade plan, which must accommodate the basic functions (mission) of the site while still meeting the objectives of enhanced security. Adjustments and compromises may have to be invoked in

considerations regarding work procedures and processes, safety, security regulations, and other factors and constraints. The design process begins by considering alternative countermeasures to address each vulnerability. Then, the principal functional features of physical environment, facilities,

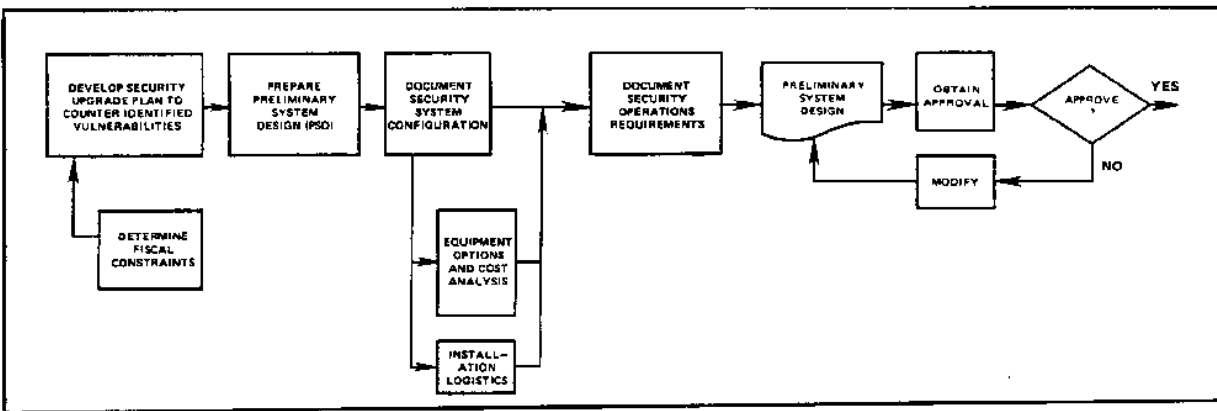


Figure 12
Phase 2 - Preliminary System Design

barriers, and sensor subsystems and their performance characteristics are considered. Specific combinations are considered in terms of complementary functions and supplementation of performance capabilities. For example, intruder detection may be provided by point and space protection sensor elements, or physical barriers may be used in conjunction with interior and exterior detection sensors and area surveillance devices. The combinations provide a synergistic effect in burdening the adversary by requiring special equipment and by adding to penetration delay times. See DM-13.01 for additional information regarding delay time considerations.

3.5.4.1.1 Determine Fiscal Constraints. Fiscal constraints are factored into the equation early-on to provide pragmatic limits on design alternatives. Security practitioners must devise a security upgrade plan in consonance with these many constraints, and at the same time, reduce the probability of successful adversary penetration. The results of the consequences analysis and consensus steps in Phase 1 can directly serve the interests of good judgment at this juncture.

3.5.4.1.2 Preliminary System Design (PSD). The conceptual design proceeds to the preparation of a more definitive security system design. A system configuration complete with identifiable subsystem and subsystem elements can now be set forth. A variety of alternatives may still be available. For example, if the design basis threat is an insider adversary in collusion with outsiders, the mix of procedural, access control, and subsystem redundancy features will still be under active debate. Hardware versus personnel intensive solutions may look equally attractive during early stages of PSD development depending upon threat and vulnerability requirements. A principal set of considerations during intrusion detection subsystem discussions will invariably surround the issues of nuisance alarms and probabilities of detection of various electronic sensor configurations. Site-unique environmental data generated during Phase 1 assessments will provide specific input affecting the candidacy of various phenomenologies and the site preparation required for potential applications. Design basis threat data will directly assist in the determinations of operational requirements for probability of detection success. In many cases, the use of multiple and diverse sensor arrays, logically combined, in conjunction

with redundant power

13.02-26

and communications capabilities will provide the necessary defense-in-depth at various zones throughout the protected area.

3.5.4.1.3 Phase 2 Summary. Cost analysis (both initial and life cycle), logistics involved in system options, and the operational enhancement features of alternatives assist in the development of a "best" solution to satisfy the unique requirements of the site. The final preparation of the PSD provides the user with a comprehensive overview of how the proposed system will both counter the design basis threats identified and mesh with required user operations. Similarly, the policy implications involved in system implementation are provided in the overview: present and future cost of the system or system options and the consequences the user can avoid. Lastly, the PSD informs him that he may proceed with system implementation with assurance that the design represents an optimal solution given the resource commitments approved by decisionmakers.

3.5.5 Phase 3 - Preparation of Final System Design. The final system design (FSD) phase sets the security system design process into a preimplementation cycle and takes the preliminary system design to the levels of specificity required for actual procurement and installation (see Figure 13). It is during this phase that all of the many steps required for subsystem and subsystem element implementation are identified, individual task/event and cost/schedules are prepared, performance specifications to the element level are drawn, and required facility renovation/construction plans are developed. A critical element in this phase is synthesis: preparing a system integration plan which takes each individual component and specifies its placement, interrelationship, and contribution to overall, integrated system performance. The sum of the parts are specified at this point and the totality can be viewed as an integrated whole. If this synthesis step could be viewed as a matrix, the horizontal axis would be seen as the columns of subsystems set forth in Section 2 of this manual, The vertical axis would break down each location (or sector) of the site (e.g., access points, building perimeter, specific interior locations, etc.). Each column would indicate subsystem elements required for deterrence, delay, detection, and

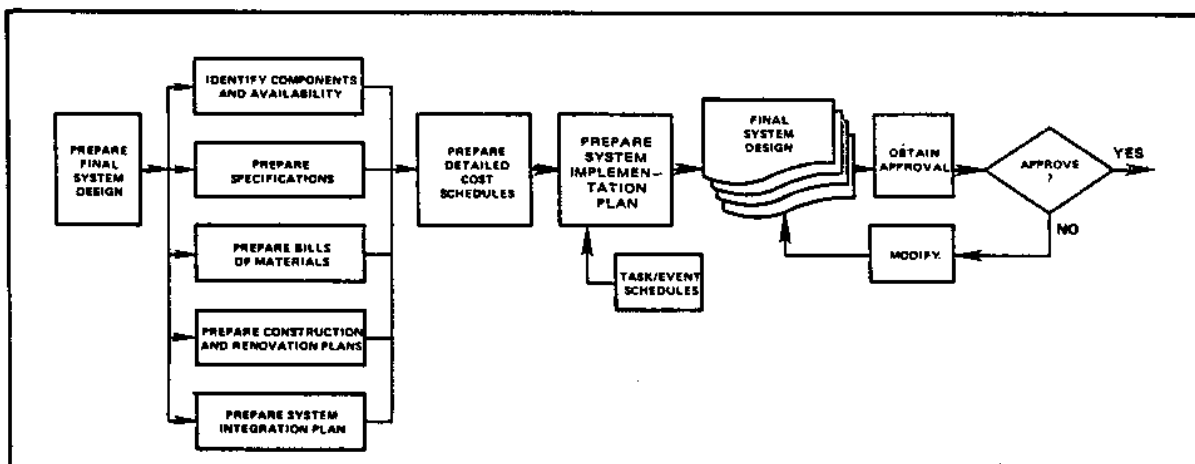


Figure 13
Phase 3 - Final System Design

response/operation given the design basis threat(s) postulated in Phase 1. With the identification of each subsystem element required for the FSD, a system implementation plan can be prepared with supporting documentation. A feedback process is incorporated for end user review and approval.

3.5.5.1 Preparation of System Design Documentation. It is essential that system design documentation developed as outputs to the security system design process be consistent with the project schedule and applicable NAVFAC documentation requirements. Two basic project types establish the requirements for these deliverables: (1) the security system is a stand-alone, retrofit, MCON, or O&M project at an existing facility; or (2) the security system is an integral part of a large MCON project at a site under design. In the former instance, the design documentation is keyed specifically to generation of engineering and procurement-related details required for installation of an operational security system. In the latter, the security design documents are but a part of a total design package which must be integrated in form and content with outputs of other contractors or divisions.

3.5.5.1.1 Preliminary Engineering Stage. This stage consists of engineering studies, concepts, or Project Engineering Documentation (PED) preparation necessary to ensure that requests for authorization and funding of construction is on an economically sound basis. The result of this stage is economic and functional justification of a proposed project and will normally comprise (1) a predesign conference, (2) a preliminary system design incorporating red-lined drawings of proposed system locations and elements, and (3) preliminary material lists and cost estimates. If required, early in the Phase 1 description provided earlier, Military Construction Project Data (DD Form 1391) may also be developed for Program Objective Memorandum (POM) input for the Navy.

3.5.5.1.2 Project Design Stage. This stage consists of the development of detailed drawings, specifications, and cost estimates for authorized military construction projects and/or repair or improvement projects. The PED provides the conceptual basis; this stage normally comprises three or four submittals: (1) the 35 percent design with requisite analyses regarding threat, specific vulnerabilities, and security system requirements. These reports should be evaluated individually for requirements regarding security classification. Preliminary drawings of site improvements and security component location, system and subsystem option diagrams, and preliminary material lists and cost analyses provide a foundation for discussions with user activities, public works, or others as required for consensus on system direction and cost/performance implications. Normally, the NAVFAC design process requires preparation of an outline specification, but in the more complex system designs, the final selection of specific technical solutions may not be sufficiently fixed at this first phase of the Project Design Stage, (2) the prefinal submittal is at about the 90 percent phase and the design will be essentially complete with final drawings, specifications, schematics, scope of work, material lists, and cost analyses in a format established by NAVFAC guidance. If commercial equipment is to be specified, NFGS-16727, Intrusion Detection Systems (IDS), will form the basis of this document. If military equipment is specified, appropriate technical guidance should be sought from

NAVELEX and/or the applicable organization responsible for each equipment item, (3) the final submittal (100 percent) consists of the prefinal documentation as modified by corrections and clarification comments received from reviewing user and/or NAVFAC activities. Deliverables include original tracings and two sets of prints, one bound manuscript, two bound copies of the final specification, and three sets of the project cost estimates.

3.5.5.1.3 Classification. Most NAVFAC project design documentation is not classified. Use of a cleared contractor for security projects, however, is recommended by OPNAVINST 5530.14, U.S. Navy Physical Security Manual. The classification of documentation, such as vulnerability analyses, record drawings, etc., will normally be determined by the using activity but, as a general rule, no physical security project is classified higher than SECRET. If possible, 100 percent submittals should be unclassified, but record drawings may be classified. This may preclude the requirement for a cleared construction contractor. When support services are required for a classified project, care should be taken to select an A/E firm with a DoD clearance. This requirement for classification, however, may add to procurement time for both the A/E services and in the construction contract. Similarly, classification requirements place an additional administrative burden on NAVFAC due to required document control procedures.

3.5.6 Phase 4 - System Implementation. The system acquisition, installation, and acceptance phase is perhaps more critical to system performance than any preceding phase. It is at this stage of the process that the system designer can lose control of the desired results. Project implementation controls need to be extended from the specifications throughout this fourth phase to ensure that quality assurance is built into each step of the post-design process. These steps are shown in Figure 14.

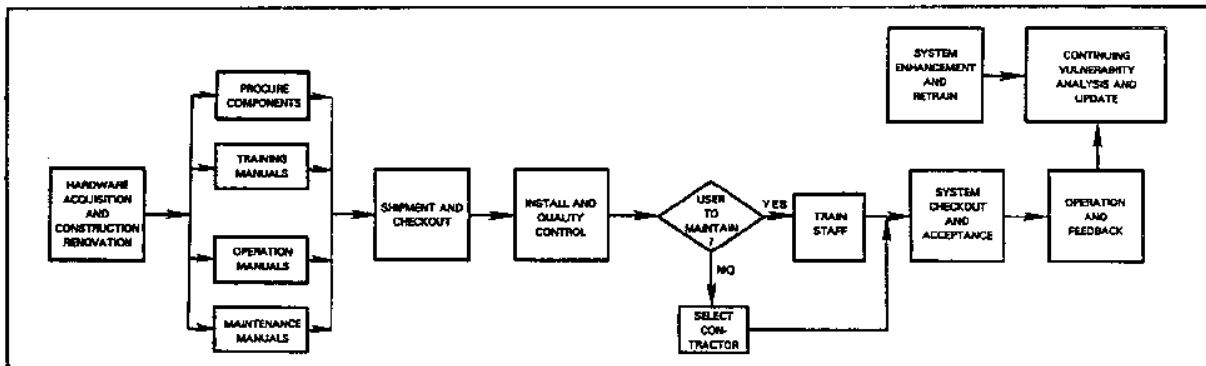


Figure 14
Phase 4 - System Implementation

3.5.6.1 Hardware Acquisition and Construction/Renovation. The installation phase commences with initiation of the procurement cycle adopted for the project or, alternatively, with construction tasks assigned to Navy activities. Typically, installation of commercial IDS will be contracted out to qualified firms who will supply, install, and maintain the system. This procurement will often be part of the electrical specifications in new construction or as a stand-alone procurement in a retrofit application. In

both cases, the specifications must be sufficiently detailed to ensure installation quality control, and the supervision of installation and test must be performed by qualified technical personnel.

3.5.6.2 Security System Acquisition. The Federal Acquisition Regulations require agencies to solicit offers, establish terms and conditions, and select contractors using two principal methods: formal advertising and negotiation.

3.5.6.2.1 Formal Advertising. This consists of preparation and publication of an invitation for bids (IFB), submission of bids by prospective contractors, and award of a contract. Specifications in invitations for bids must be sufficiently detailed and descriptive to permit full and free competition. Advertising presumes a specification that dictates a common base-line of technical features and contract terms. This obviates the need for discussions with competitors about their bids and provides an objective means for distinguishing among capable competitors on the basis of price. Since price is the criterion for selection, advertising also assumes the Government's design is adequate and comprehensive, and the specifications developed during the design phases are accurate enough to permit bidders to cost and provide the products and services within budgeted limitations. Military and civilian statutes provide that formal advertising is the preferred method of procurement. There are, however, 17 statutory exceptions to the advertising preference in military procurement, several of which are conceivably applicable to the implementation of sensitive security system installations.

3.5.6.2.2 Negotiation. If the formal advertising method of procurement is not feasible and practicable, procurement may be negotiated. Offers still must be solicited from the maximum number of qualified sources. The single element distinguishing negotiation from advertising is the subjective judgment which weighs quality and other factors against price. If the detailed design process described throughout the prior phases is followed, the result will be sufficient for procurement action via formal advertising. The decision regarding negotiation tends to turn upon the presence of qualitative versus price-only determinations and/or the existence of one or more of the statutory exceptions authorizing negotiation.

3.5.6.2.3 Qualitative Versus Price Factors in Contractor Selection. Recognizing that price will determine selection in the formally advertised IFB process, it is critical that qualitative elements be incorporated within the bid request documentation. Within limits established by the Government's Contracting Officer, these should include the following criteria: (1) personnel/facility clearances in accordance with DoD security requirements, (2) technically qualified corporate and staff experience with technologies proposed, (3) experience in installations of similar size and complexity, (4) logistic capability to meet timetables and performance requirements.

3.5.6.3 Installation Observation, Inspection, Test, and Acceptance. The on-site quality control of security system installation is deemed essential to system performance. Depending upon the sensitivity of the project, various levels of on-site observation and inspection of implementation tasks at key phases of preparation, wiring, installation, and test are critical to Government acceptance of operational systems. In the most sensitive sites, security during construction is often a DoD requirement to ensure that covert devices are not emplaced or system components bypassed during these phases where the site is open to outsiders. The design process in earlier phases needs to consider carefully the key points in the installation management of each project where on-site inspection can confirm that system design requirements are being met by the contractor(s). Personnel utilized in the performance of these tasks should be completely familiar with the devices being installed and the technical requirements for proper installation and testing. Field inspections and tests performed by the contractor should be closely monitored by the Government and field inspection and test reports prepared at the conclusion of each such task. Shop drawings, as-built drawings, and other deliverables required of the contractor by the specifications or contract terms should be reviewed for acceptability and quality control. Formal acceptance of installed systems should only be made after Government confirmation of all quality control provisions contained in the specifications. The burden of proof of system performance is upon the contractor.

3.5.6.4 System Documentation. Specifications will necessarily include the requirement for preparation of a variety of documents pertaining to the installation, maintenance, and operation of the system. This is particularly true of large, multi-subsystem configurations involving a guardforce interface at an alarm control center. The system supplier may be required to submit shop drawings, as-built drawings, logistics support plans, installation and maintenance instructions with parts breakdown, system operation manuals, and training plans and documentation.

3.5.6.5 Post-Implementation Tasks. The turnover of installation systems cannot be seen as the end of the implementation process. Because threats are dynamic, the capabilities to meet newly identified requirements must be assessed periodically. Changes in facility function or operational routines may alter the previously acceptable location of entry control devices, sensors, cameras, or other components. Maintenance of installed systems and routine testing for performance are absolutely critical and should be documented. If contractors are used for system maintenance and repair, a closeout inspection of the work and restored performance of the device or element is always a requirement.

Section 4: TYPES OF SENSORS

4.1 Point Sensors - Interior. Point sensors are devices normally employed to protect particular locations on the perimeter of a structure or particular objects or locations within a structure. By definition, they are not capable of providing detection capability within a volume of space, although conversely, some volumetric sensors may be applied for point protection. In many applications, point sensors are used by themselves to provide a basic level of intrusion detection. For higher level security requirements, they should be employed in conjunction with other sensors such as volumetric sensors. Generally, point sensors can be bypassed by a skillful and knowledgeable intruder.

4.1.1 Door and Window Protection. Doors and windows, the primary openings in a structure's perimeter, are also the primary points of intrusion attempts. Many times, protection of these obvious portals is the first consideration of the security system designer. Most DoD and USN directives which require IDS also require, as a minimum, that structure portals receive IDS protection. Point sensors used for door and window protection use very mature technologies and are highly reliable if installed properly. Because they have been used for many years, however, potential intruders with a relatively low level of sophistication are thoroughly familiar with them and their weaknesses. For example, many types of point sensors providing protection for doors and windows sense the interruption of a continuous flow of low voltage electric current or electromagnetic field. If an intruder can enter through the portal without causing an interruption in the electrical circuit, such sensors will be bypassed successfully. Improper placement in sensor installation often contributes to such a vulnerability. Consequently, the design basis threat's capabilities, the level of security required, and the principle of defense (protection) in depth should be considered in the application of point sensors for portal protection.

4.1.1.1 Balanced Magnetic Switches. Also referred to as door "switches" or "contacts" or "magnetic contacts," this sensor is the most commonly used intrusion detection device. As a switch, this sensor incorporates electrical contacts that make or break an electrical circuit as a result of physical movement. The standard magnetic switch sensor consists of two components, each housed separately. One of the housings contains the contacts which will open or close in the presence of a magnetic field. The other housing contains a magnet to provide the required magnetic field. The magnet is mounted on the inside (protected area side) of the portal component which moves (e.g., door, window), and the switch is mounted on the inside frame (see Figure 15). When the magnet is removed from the vicinity of the switch (e.g., door is opened), the switch activates (see Figure 16). The amount of movement required is generally less than 2 inches. Certain DoD and USN directives require as little as 1 inch maximum separation for switch activation; others require switch activation prior to visual access or the capability being achieved to physically access the sensor. Since the switch contacts are held in their

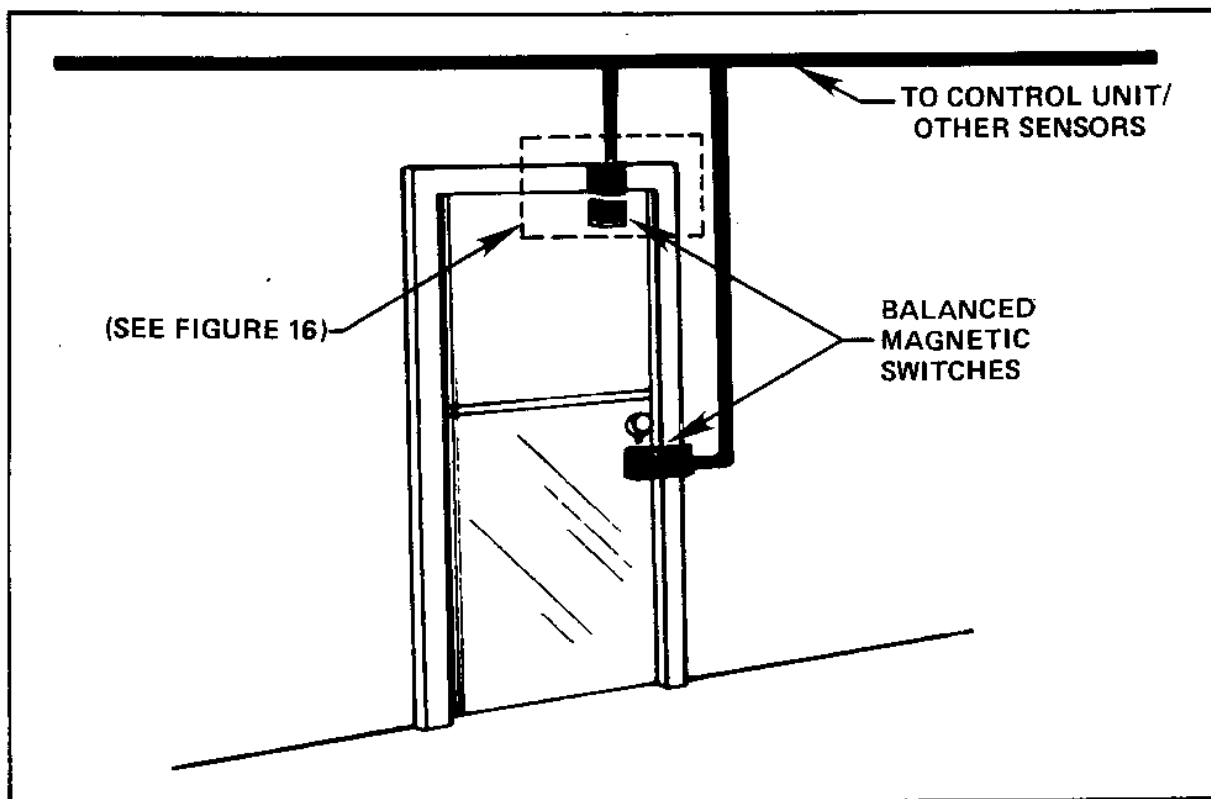


Figure 15
Standard Magnetic Switch Application

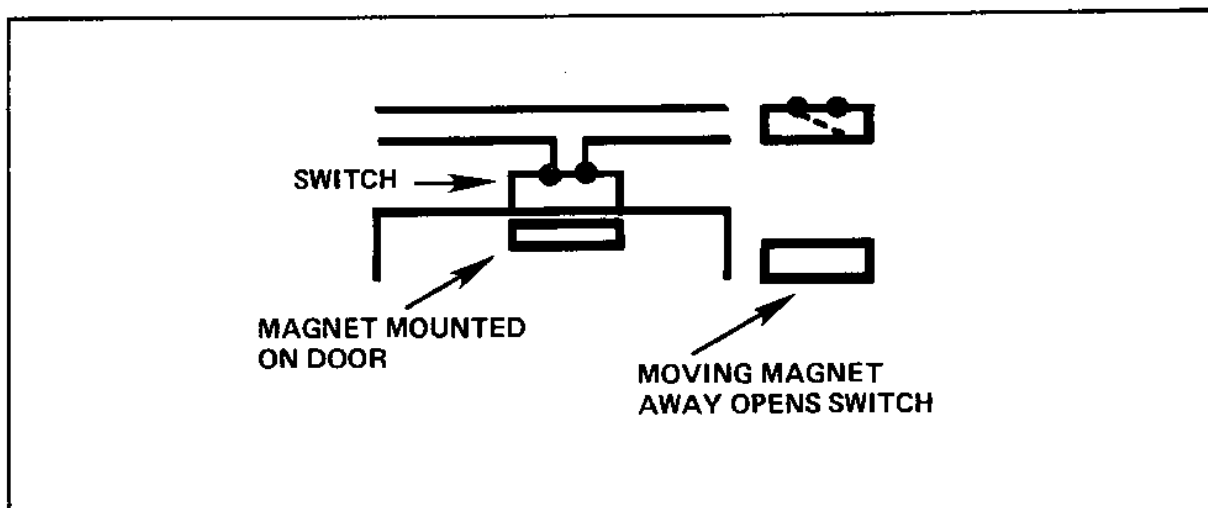


Figure 16
Standard Magnetic Switch Application (Enlarged View)

normal position by the magnet, it is possible to defeat a "plain" magnetic switch by placing a strong magnet near the switch, thus preventing the contacts from actuating when the normal switch magnet is moved away (e.g., door opened). For this reason, the only acceptable type of magnetic switch for most DoD applications is the balanced (or biased) magnetic switch (BMS). BMSs are available in both surface mount and recessed configurations and in many model and style variations. Surface-mounted models for high security applications must be equipped with tamper alarm protection. Recessed models are inherently protected against tampering since the actual door frame must be attacked first to gain access to the switch components. The following application and installation considerations apply to BMS:

a) Biased Magnetic Switch. This switch consists of one reed switch with a biasing magnet that changes the state of the reed switch. The actuator magnet is then placed at the correct distance to offset the bias magnet, creating a "balanced" condition. This type of switch can be defeated with the use of a single magnet, but the person must have the correct size magnet, correct polarity, and must not bring the second magnet too close to the switch. Correct installation of the actuator magnet is essential. It could be defeated by an expert using a single magnet of the correct size and polarity and placed in a critical location.

b) Balanced Magnetic Switch. This switch consists of one biased reed switch and one unbiased reed switch. The second reed must be of the correct sensitivity and position to not operate with the actuator magnet. It must operate with the addition of a second magnet. This type switch requires an adjustment of the actuator magnet at the time of installation and should be periodically checked for adjustment. It could be defeated by an expert using a single magnet that is moved into place as the door is opened. This would require a coordinated movement of the door and magnet from inside the protected area.

c) Preadjusted Balanced Magnetic Switch. This switch consists of three biased reed switches and may have an optional fourth tamper reed. Two reeds are polarized in one direction and the third is polarized in the opposite direction. Steel is built into the switch so that mounting on steel will have no effect during installation and the adjustment will remain correct. The magnet housing consists of three magnets with the polarity that corresponds to the switches and also has steel backing. The unit is preadjusted to have a fixed space between the switch and magnet. Field adjustments are not possible or necessary. This switch is for applications which require the highest degree of security. The unit with three reeds could be defeated with one of its own magnets, but not a bar magnet. The unit with four reeds cannot be defeated with either a bar magnet or another actuator magnet, since the tamper or fourth reed will activate when the actuator magnet or any other magnet is brought within actuating distance.

d) Door type and fit are important considerations in BMS model selection. Doors may tend to move due to wind or internal changes in air pressure. If this movement is excessive, BMSs will produce nuisance alarms. The choice between surface mounted or recessed BMS may be governed by door

type, fit, and aesthetics. The position of a surface-mounted BMS is relatively easy to adjust during final installation to accommodate variances in door type and fit, whereas recessed models are relatively difficult to adjust. There may be a cost-effectiveness limit on door type selection and fit adjustment that may dictate BMS type selection. For new construction contracts, doors and frames for recessed BMS should be specified to be procured with the appropriate recesses already in the doors and frames.

e) Applying a BMS where not required, as a "nice to have" feature, should be avoided. Overapplication of any sensor, despite its reliability, increases maintenance requirements and the likelihood of false or nuisance alarms. On the other hand, not applying a BMS where required may produce an unnecessary vulnerability into the security system design. The system designer must keep in mind that a BMS detects movement of a portal but does not detect movement within a space.

f) A BMS which is not securely mounted can have sensitivity loss or cause nuisance alarms after repeated portal opening and closing. Good mounting hardware and proper installation techniques will minimize such problems. Assuring correct polarity alignment is particularly important for a recessed BMS.

g) If multiple BMSs are required for a particular application, they must be installed carefully to avoid an improper connection, which may result in two leads having a "jump" between them, rendering the sensor(s) inoperative.

h) Glass encapsulated reed BMSs must be handled with care to preclude inadvertent damage. These are particularly suitable for highly corrosive environments.

i) Some models of BMSs have a minimum separation as well as a maximum separation required between switch and magnet housings. To maximize performance, installation requires use of an ohm meter. The meter is attached to the switch leads. Moving the magnet housing toward and away from the switch will, by marking the two positions where the meter indicates the switch has activated (0 ohms for a switch closure), indicate the maximum adjustment range possible so that sensitivity can be properly adjusted by correct positioning of the housings.

j) Performance testing of BMS should be conducted with other sensors in the protected space deactivated so that, for example, faulty BMS performance is not masked by a volumetric motion sensor sensing a portal opening.

4.1.1.2 Glass Breakage Detectors These sensors are used to detect breakage of glass by an intruder who is attempting to enter a portal by bypassing security hardware (e.g., lock) or IDS devices such as the BMS.

The generic types of sensors normally applied for glass breakage detection are discussed below. Volumetric sensors may also be used in the vicinity of the interior window area to detect the intrusion rather than the actual glass breakage.

a) Breakwire. This type of sensor generally functions in the same manner as foil. The breakage of glass also causes the breakage of thin (No. 24-36 AWG), low tensile strength (maximum 4 pounds) wire, imbedded in window mullions or overlaid on the glass itself, which interrupts a low-voltage direct current running through the wire producing an alarm. Another form of this type of sensor is the application of a "trip wire" on the inside of the glass area. Movement or breakage of this wire causes an electrical current to be completed or, in another form, to be interrupted, producing an alarm. The simplicity of this sensor makes it highly reliable but also makes it relatively easy to defeat by jumping or bridging the wire circuit and then cutting through it. Several application and installation considerations apply to breakwire sensors as well. Because an unsophisticated intruder can defeat this sensor with relative ease, it is not found in most DoD applications. It is suitable for relatively low level security applications such as quarters, convenience stores, etc., but should be used in conjunction with another sensor (preferably a volumetric motion detection sensor) to assure intruder detection if defeated or bypassed. Generally, a breakwire sensor is used in a different application for DoD facilities as "wire trap" for building vent and duct protection. Interlaced in such an opening, it provides effective protection and is not visible (and hence not vulnerable) when used for window and other glass protection. This sensor may be used also for protection of other portals. Its use in providing protection for overhead doors, for example, is one application. Fourthly, when specifying installation as a "trip wire," the wire normally used as the trip wire should be substituted during daylight. The use of blackcoated wire, deployed only at night, also increases effectiveness. Lastly, the man-hours involved in properly positioning and installing a breakwire sensor, depending upon the application, far exceed the cost of the sensor. Careful consideration of the tradeoffs involved must be a part of the system design process. Another type of sensor which costs more, but takes less time to install, may be more cost-effective.

b) Vibration/Ultrasonic. This category is two separate sensors. However, since their outward appearance is identical and they are used for the same application, both vibration and ultrasonic glass breakage sensors will be covered in this section. Both types are also known as "window bugs;" vibration sensors are also called "shock" sensors. Vibration sensors detect attempts to penetrate building perimeter barriers, such as a window, by sensing with a piezoelectric crystal the intense vibrations which are associated with intrusion attempts. Normally, the better quality sensors of this type have a sensitivity adjustment with a relatively extensive range (e.g., one complete turn potentiometer) and mechanical filtering. This assures minimal nuisance alarms due to flexing of glass and other nuisance sounds such as heavy construction or traffic. Ultrasonic penetration detection sensors detect the sounds made by a forcible intrusion attempt even if these sounds are barely audible or inaudible to the human ear. They are "passive" receivers and should not be confused with active ultrasonic motion sensors discussed elsewhere in this section. These sensors consist of a

microphone and an electronic processor which discriminates between "noise" such as human speech and the specific frequency associated with a forcible intrusion attempt. Both types of sensors are relatively low profile and easy to install. They are difficult to defeat. Type selection depends upon the propensity of the ambient environment to produce nuisance alarm stimuli.

4.1.1.3 Application and Installation Considerations. Several application and installation considerations apply to vibration and ultrasonic penetration detection sensors. For one, vibration sensors should not be applied in situations where high vibrations are encountered such as on shipboards, in proximity to heavy construction, on a railroad, or in heavy vehicular road traffic. They cannot be used effectively outdoors, and they do not function well on plastic or polycarbonate sheets. Both types of sensors are relatively maintenance free when applied and installed properly (including sensitivity adjustment) and are distributed by most quality sensor manufacturers with an integrated battery backup. These sensors should not be applied singly to cover an area (of glass) greater than 6 feet square and should be applied in pairs to cover large areas (see Figure 17). For multipane applications, two sensors should be specified to be applied to the midpoints at the top and bottom of the area. Some portal configurations, such as double hung or crank-out windows, dictate application of the sensor(s) on the window of frames to provide effective coverage. Lastly, testing and adjustment is usually accomplished with the use of a "test device" consisting of a string-suspended ball which is allowed to swing against the perimeter barriers (e.g., window pane) to simulate a forcible intrusion attempt. This device, or a tuning fork for ultrasonic sensor adjustment, is often offered as an extra cost option by a "window bug" vendor. A low cost but effective alternative is to use a ring of keys swung against the barrier (e.g., glass) as the adjustment stimulus.

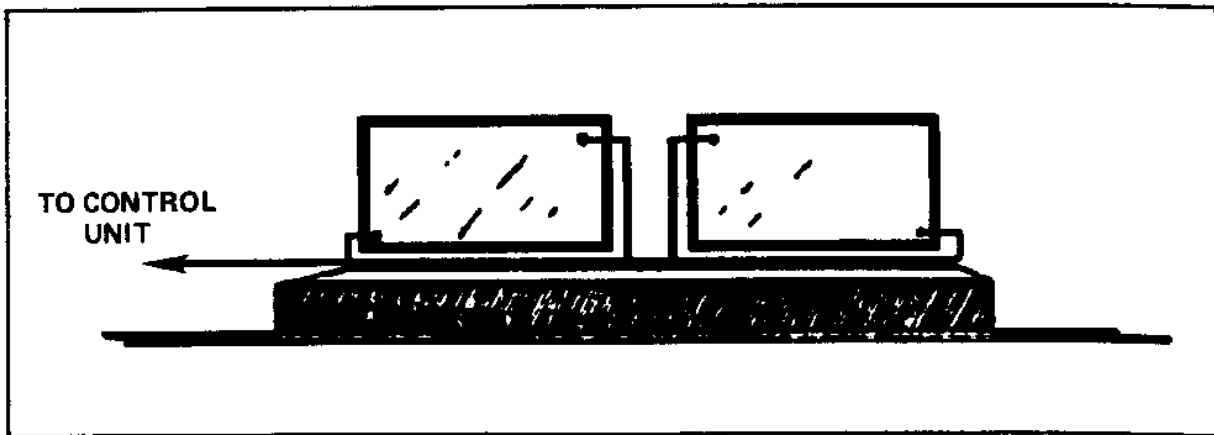


Figure 17
Vibration/Ultrasonic Glass Breakage Sensor Application

4.1.1.3 Screening and Detection. Metallic screening or grating can be used for window and other portal physical and intrusion detection protection. Use of screening consisting of breakwire sensor type wire, functioning in the same manner (electric circuit interruption) as a breakwire sensor, is an effective application. To be effective, the entire area must be covered (such as both halves of a double-hung window) and anchored to the building to minimize the possibility of bypass. Recessed BMS can be employed to detect movement of removable screening in separate frames. Larger grating can be protected by fence sensors or by capacitance proximity sensors as discussed later in this section. The considerations for application and installation are the same as for the breakwire sensors discussed above and for the applicable fence and capacitance proximity sensors discussed later in this section.

4.1.2 Object Protection. Some applications require the protection of individual objects within a space rather than protection of the entire space. This is often dictated by operational procedures or cost constraints. This section provides a discussion of both sensors designed specifically for object protection and the application of other sensors for that purpose.

4.1.2.1 Capacitance Proximity Sensors. This type of sensor is specifically designed for protection of an individual object or series of individual objects within a relatively small area. The only restrictions are that the object be metal and insulated from an electrical ground. Successful applications have ranged from safes and file cabinets to vehicles and aircraft. Capacitance sensors establish an electrostatic field on an object and monitor the capacity for electrical energy storage between a specific metal object or a series of objects and an electrical ground. Any disturbance in this capacitance, caused by someone or something touching the object, causes an alarm. Sensitivity adjustment permits extension of the capacitance field to the close proximity of the object surface or limitation at the object surface depending upon the application. The better quality capacitance proximity sensors automatically adjust to small changes in the capacitance of the protected object(s). The following application and installation considerations apply to capacitance proximity sensors:

- a) Capacitance proximity sensors are relatively insensitive to environmental factors which may adversely affect volumetric (space) protection sensors.
- b) Objects to be protected must be isolated to preclude grounding.
- c) Figure 18 depicts an application of a capacitance proximity sensor to a series of objects. Note where the system is grounded and the relatively large end of line resistance (minimum 10k ohms) required.
- d) Capacitance proximity sensors may be used with grid wire or screening (breakwire) sensors. However, this application is infrequent since

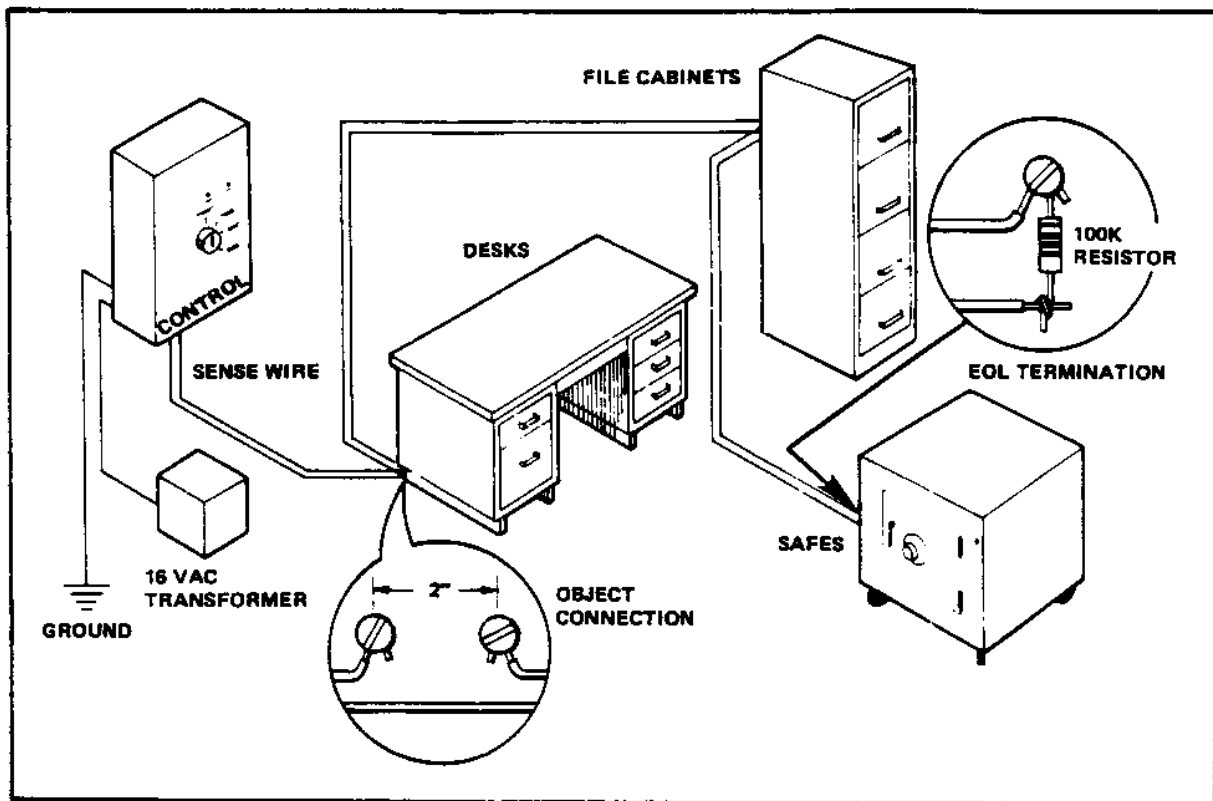


Figure 18
Capacitance Proximity Sensor Application

the additional protection provided is generally offset by the increase in nuisance alarms.

4.1.2.2 Application of Volumetric Sensors. Volumetric sensors are sometimes used for object protection. The types used for such applications are generally restricted to those whose energy can be focused or limited to coverage of the individual object(s). Passive infrared sensors are used frequently. Ultrasonic sensors are used sometimes for object protection within a confined area. Because of the difficulty of limiting the energy, microwave sensors are used seldomly for this application. However, several bistatic microwave or photoelectric sensors may be used to establish an electronic "fence" around an individual object. The effects of environmental conditions, the difficulty of restricting sensor energy to the object(s) involved, and cost are important tradeoff considerations in deciding to apply a volumetric sensor to object protection. Capacitance sensors are designed for this purpose; volumetric sensors are not. Often, the application is dictated by whether or not the protected object is metal and can be effectively isolated from ground.

4.1.2.3 Pressure-Sensitive Sensors. Also called pressure mats, this sensor consists of switch(es) enclosed in a mat which are normally placed at approaches to areas containing objects requiring special protection. Mats vary in sensitivity from 5 pounds to 20 pounds per square foot and may be cut to fit the area of application. Activation of the switch causes an alarm signal to be transmitted via the connecting wires (which should be concealed) to a control unit. The following application and installation considerations apply to pressure-sensitive sensors.

a) Positioning is critical since these mats, normally only the width of a stair runner, may be easily stepped over. They should be concealed and positioned where someone approaching the protected object would have to step, for example, just inside door openings, under stair runners, or under a carpet immediately surrounding the protected object.

b) Plastic-encased versions should be specified to preclude failure due to dampness or high humidity. Sealing connections in epoxy will help avoid such failures.

c) These sensors can be extremely cost effective when purchased in bulk rolls. Properly positioned, they offer good protection against an unsophisticated intruder.

4.1.3 Floor, Wall, and Ceiling Protection. While most unsophisticated intruders take the most obvious approach to attempt an intrusion, an intruder who is knowledgeable of the presence, capabilities, and limitations of IDS elements protecting portals may attempt to bypass this protection and obtain entry through other parts of the building perimeter (floors, walls, or ceilings). The sensors discussed in this section are specifically designed to detect such forcible intrusion attempts.

4.1.3.1 Vibration Sensors. Also called "shock" sensors, these sensors operate as described in "Vibration/Ultrasonic" and the same considerations for application and installation apply. Other considerations are:

a) Figure 19 depicts the inner workings of one type of vibration sensor. Others of equal quality may use one or more balls or other "mass" devices balanced between contacts. When the electrical circuit is completed (or broken), an alarm results.

b) The simplest vibration sensor is a mechanical contact switch designed to actuate when the surface on which the sensor switch is mounted starts to vibrate. This latter type is also subject to more nuisance alarms

from sources of vibration which are not attempts at penetration (e.g., exterior vehicular traffic).

c) Rigid wall materials such as masonry or reinforced concrete make excellent surfaces for application of this sensor.

d) The sensor should always be specified for installation on the inside of the wall surface (within the protected area).

4.1.3.2 Grid Wire Sensors. Grid wire sensors are a form of breakwire sensors discussed in paragraph titled "Breakwire." In this case, the wires are arranged similar to a screen, discussed in paragraph titled "Screening and Detection," but with a larger mesh, normally not more than 4 to 6 inches square. The "grid" is imbedded in or affixed to the building perimeter barriers being protected. When the barrier is penetrated, the wire (and electric circuit) is broken, causing an alarm. The same considerations for application and installation which apply to breakwire and screen sensors apply to grid wire sensors. Other considerations are:

a) Figure 20 depicts a grid wire sensor application. Note that the connection to the door is flexible to allow opening and closing without causing strain on the connection cable.

b) When specifying installation, the wire grid should be, if not imbedded, covered with wallpaper or similar material to conceal the grid and protect it from accidental breakage.

c) Whenever broken, either accidentally or by an intruder, the grid must be repaired to restore protection.

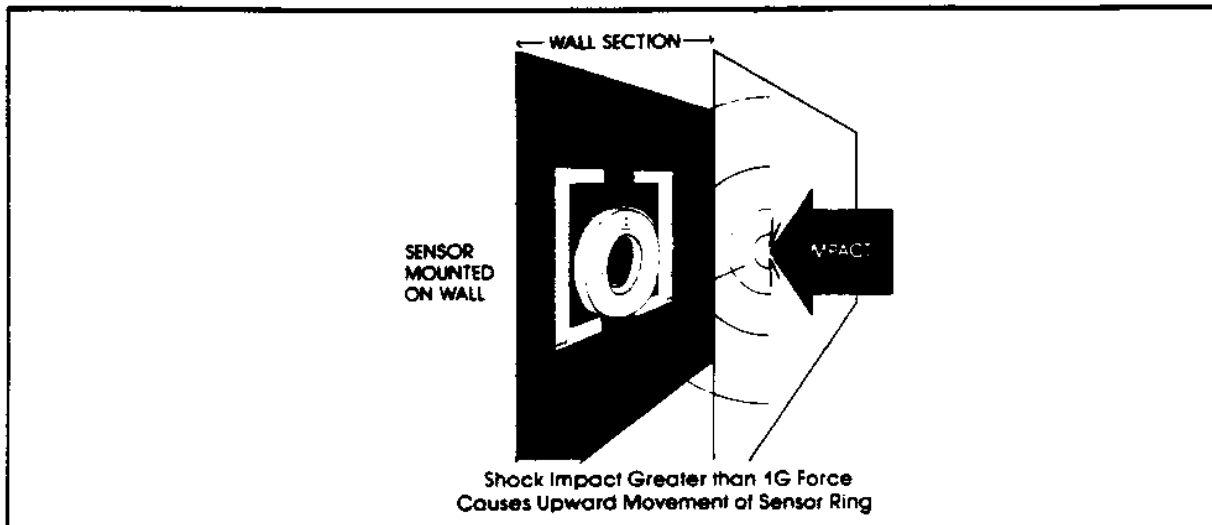


Figure 19
Vibration Sensor (Wall/Floor/Ceiling Protection)

d) The low maintenance requirements and high reliability of grid wire sensors are also important trade-off considerations.

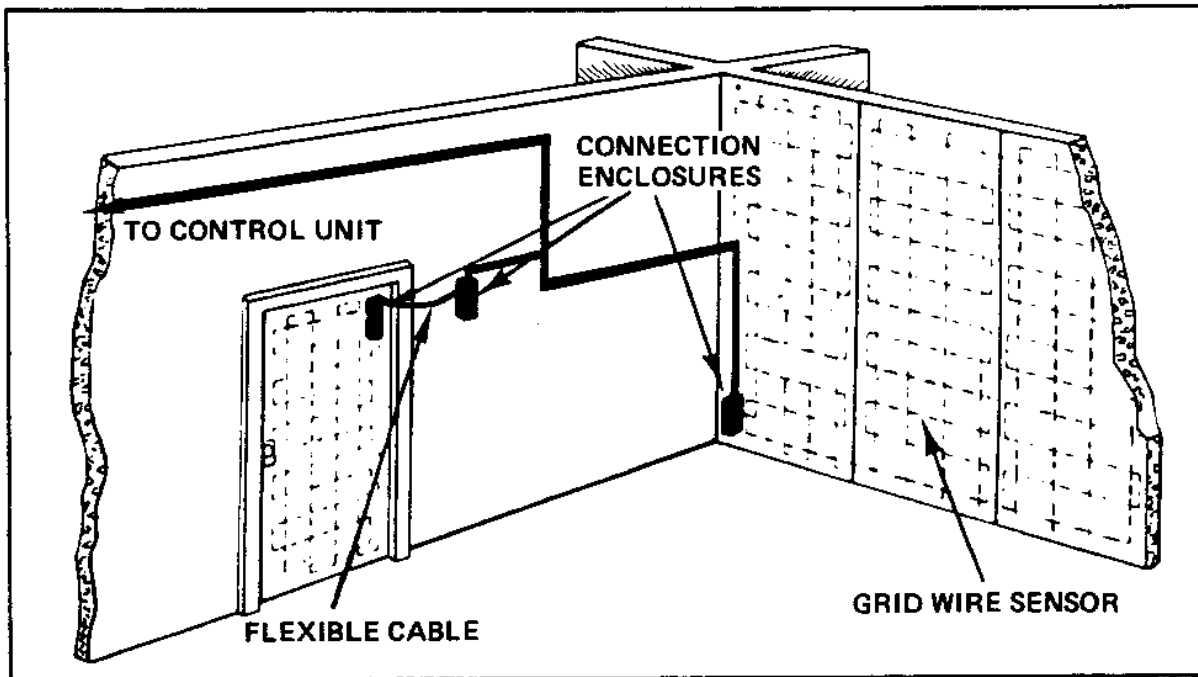


Figure 20
Grid Wire Sensor Application

e) The relatively high cost of installation (man-hours) is an important consideration in tradeoffs by the security system designer in selection of grid wire sensor versus another type for a specific application.

4.1.3.3 Protection of Utility Inlets/Opening. This application is normally accomplished by the configuration of a breakwire sensor in a laced "wire trap configuration or by the use of volumetric sensors. The use of "wire traps" for this application is discussed in paragraph titled "Breakwire." The considerations for application and installation discussed therein apply. Other considerations are:

a) Sensor type selection and application are dictated by what is passing through the utility inlet/opening (cable, air, fluid, etc.).

b) The application of volumetric sensors to utility outlets, such as duct work, is not advised due to the high nuisance alarm rate caused by the environmental control system (airflow, etc.). Volumetric sensors are usually most cost effective for protection of false ceilings, raised flooring, and other relatively benign spaces.

c) The protection of utility inlets/openings should include

application of BMS or other suitable sensors to access openings.

d) Utility inlets/openings which have open fluid flow (sewers, culverts, etc.) are challenges for the security system designer. Present technologies to apply include: BMS on access covers; electric cable fence sensors on inlet/outlet gratings; fabrication of metal gratings which do not materially affect water flow but which have a sense wire within the grating; and the use of pulsed infrared beams or other highly directional bistatic sensors above the fluid level.

4.2 Volumetric Sensors - Interior This term is used to denote a sensor which detects a change of state (normally motion) within a protected space. Some volumetric sensor types are called "active" in that they flood an area with a type of energy (e.g., ultrasonic, microwave, infrared beam) and detect a change in that energy state. Other volumetric sensor types are "passive" in that they monitor the change in state of a particular energy which exists in the protected space, e.g., heat (infrared), sound (audio), or light shades (CCTV), and detect a change in that energy state. Volumetric sensors are restricted generally to detection within a confined space inside a structure. Some models do have range limitations or other detection pattern limitations which make positioning a critical factor in determining sensor performance. The security system designer may have selected the optimal sensor for a particular application, but lack of a proper installation specification. Its improper placement, or lack of quality installation supervision, will result in poor sensor performance and poor protection of the desired area. Volumetric sensors may be used by themselves or in conjunction with point sensors or other volumetric sensors to provide a higher level of security. While very effective in proper applications, they are subject to defeat by an intruder who knows and understands what phenomena they sense and what their limitations are. Too often, misapplication of volumetric sensors or poor installation facilitates intruder success. While the highest levels of interior security may be satisfied by multiple combinations of different volumetric sensors, such sensor configurations may induce nuisance alarms through mutual interference if complementary sensors are not selected. In summary, volumetric sensors not only facilitate the task of the security system designer but also challenge him to assure proper application.

4.2.1 Infrared Sensors. These types of sensors may be active or passive. The "active" models are similar in operation to photoelectric beams and are discussed in the paragraph titled "Photoelectric Sensors." This section is limited to "passive" infrared sensors. Passive infrared (PIR) sensors function on the principle that all objects emit infrared energy or heat as a function of their ambient temperature. The sensor can detect sudden temperature change in an object or the introduction of an object with a different temperature (e.g., human body) within its field of view. If this temperature exceeds the specific level or threshold, it will cause an alarm. Since infrared energy is a form of invisible light, passive infrared sensors generally consist of mirrors or lenses and mirrors which collect the emitted infrared energy and focus it on a sensing element which converts the sensed energy into an electrical impulse. This sensing element may be a thermistor, thermopile, or pyroelectric element. Since the human body radiates in the

5-20 micron region of the far infrared portion of the frequency spectrum (approximately equal to the heat of a 50-watt light bulb), PIRs are designed to function in that frequency range to minimize nuisance alarms from visible light sources, etc. Electronics in the sensors restrict detection to a few seconds when the change in energy is first detected; the sensor then adjusts to the new state. Movement to a new location will then cause another alarm. The optics within the sensor will determine the patterns of detection provided. A single mirror will provide one "finger" of detection. Sensors which provide 180 degrees of coverage have up to 17 "fingers" of detection. Optimal detection distances depend upon the sensor model selected and sensor positioning. Figure 21 depicts typical PIR model coverages. The fingers depicted are actually three-dimensional cones and represent infrared energy receiving paths. As a passive device, no energy is emitted by the sensor. Consequently, power consumption is extremely low. Various sensor models permit surface or recessed mounting. Proper positioning will make a PIR self-protecting and minimize the opportunity for an intruder who is aware of the detection pattern of a particular model to defeat the sensor. The following application and installation considerations apply to passive infrared sensors.

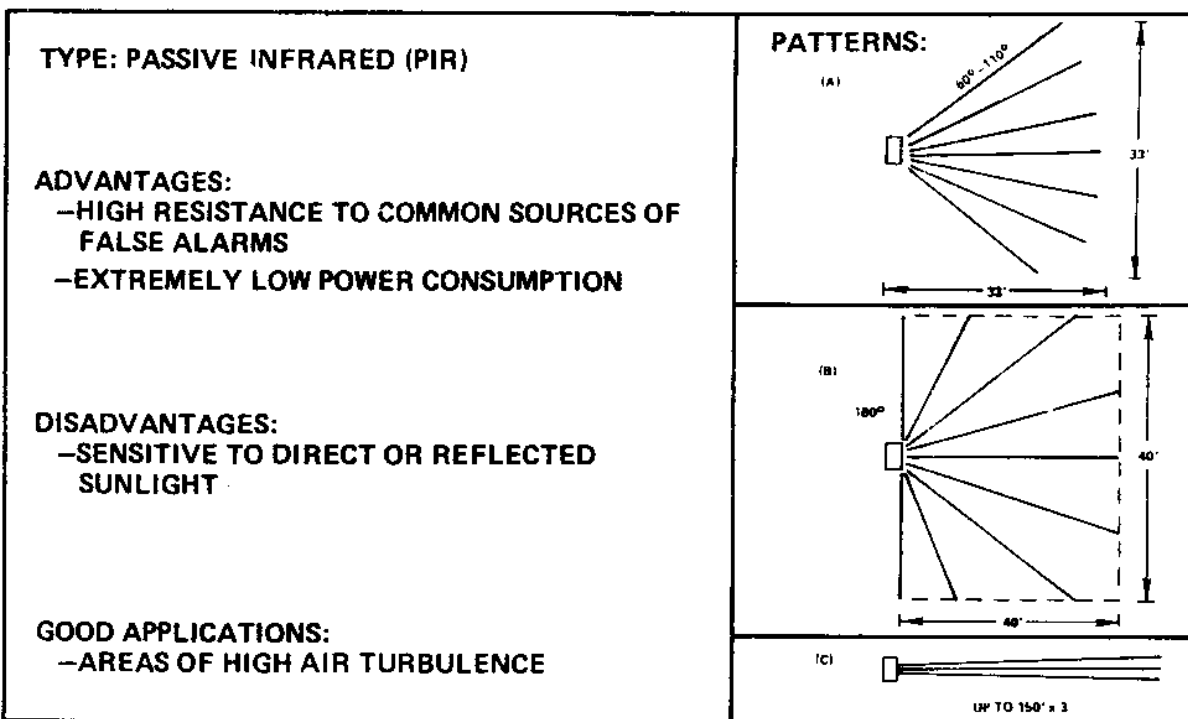


Figure 21
Passive Infrared Sensor Coverages

4.2.1.1 Considerations. Three major characteristics of infrared technology should be kept in mind by the security system designer in selecting PIRs for an application.

a) Infrared is emitted by objects because of their temperature. PIR performance will be determined by the stability of the background and the clothing of the intruder as well as his speed.

b) Infrared energy is transmitted without contact between the emitting and receiving surfaces. Viewing of direct or reflected sunlight should be avoided.

c) Infrared energy is invisible to the human eye. A PIR requires line of sight. Care must be taken in positioning so that obstructions are between receiving "fingers."

4.2.1.2 Planning Factors for Model Selection:

a) Size and shape of each area to be protected.

b) Number of areas to be covered and overlap requirements.

c) Locations where it is not possible to locate a PIR.

d) Optical and thermal environment

4.2.1.3 PIR Sensor Installation. Plan the installation so that expected intruder motion is across the sensor's field of view. The optimum mounting height is 6 to 9 feet, with primary point of aim about 18 inches above the floor on the opposite wall. Where the expected intrusion motion is toward the sensor, mount the sensor as high as practical such that it can be angled downward. This will shorten the effective range but permit the intruder to cross the sensor pattern.

4.2.1.4 PIR Sensor Location. PIR sensors respond to a change in infrared energy resulting from a rapid change in temperature. A person entering a detection area will cause an alarm signal. Sometimes a stationary object which changes temperature rapidly, such as a light bulb which fails, can cause an alarm. To avoid this, care must be taken in locating and aiming the sensors.

4.2.1.5 PIR Sensor Positioning. The infrared energy to which the sensor responds does not pass through glass or other building materials. However, intense sunlight passing through glass and shining on the sensor may cause an alarm. A metal wall or a window exposed to solar heat changes can cause an alarm. The sensor should be positioned such that direct sunlight or solar-heated walls are not in its field of view. Reflection from dark, shiny surfaces should also be avoided. A PIR should be positioned to prevent the

receiver "fingers" from having any heating or air-conditioning devices within its field of view. Positioning is critical in order to achieve optimum PIR performance.

4.2.1.6 Advantages of PIR Sensors. PIRs are often selected for areas where EMI/RFI is a consideration, yet high security is a requirement. This is because PIRs are passive devices which, if properly positioned and installed, provide optimum protection since they are relatively immune to the environmental effects which often degrade the performance of other volumetric sensors.

4.2.2 Ultrasonic Sensors. This discussion is limited to "active" ultrasonic volumetric sensors. "Passive" ultrasonic sensors which are used to detect glass breakage penetration were discussed in paragraph titled "Glass Breakage Detectors." This sensor is termed "active" because it has a transmitter which emits ultrasonic energy (inaudible to the human ear) and sets up a "standing" energy field which is sensed by a receiver. The transmitter and receiver are normally located separately within the protected area, but may also be collocated within one unit called a transceiver. As depicted in Figure 22, the transmitter and receiver locations determine the coverage pattern. This type of sensor works on the Doppler principle; movement within a stable energy pattern or field will produce a detectable change of state. Any change in the frequency of the "standing" energy field will be detected by the receiver and cause an alarm. The energy field is normally sound waves at a frequency of about 19.2 kHz per second (19 to 35 kHz are manufactured). Electronics within the sensor permit adjustment of the detection alarm threshold. Thus, the sensors can distinguish electronically between movements of a small object, such as a bird, and larger motions of a human. While the motion produced by a human will cause an alarm, these sensors can compare electronically what is transmitted versus what is received and can also make limited allowances for such sources of nuisance alarms as ambient environmental changes. Normally, the electronics are adjusted to declare an alarm with a human intruder moving at one step per second for not more than four steps. The ultrasonic energy will not penetrate, but is reflected by walls, glass, and other objects so that an intruder will be shielded. Hard surfaces will reflect the energy and extend the area of coverage; soft surfaces will absorb the energy and reduce the coverage area. Because of masking or absorption, multiple units may be required to achieve the coverage required. While the energy pattern is easily contained, the big drawback of ultrasonic sensors is that air turbulence and other environmental effects produce nuisance alarms. Areas with large volumes of moving air, such as from Heating, Ventilating, and Air-Conditioning (HVAC) systems, may be unsuitable for application of ultrasonic sensors. Slow-moving intruders or a highly sophisticated intruder can defeat an ultrasonic sensor, especially a sensor not optimally positioned and adjusted to compensate for the ambient environment. The following other application and installation considerations apply to ultrasonic sensors:

a) The sensor should be applied to a stable surface and the pattern should avoid objects whose surfaces can vibrate. To obtain maximum efficiency, aim the sensor as closely and directly as possible to the objects requiring protection.

b) Installation should never be specified higher than 12 feet above the floor on a wall; less than 10 feet is preferable. For ceiling-mounted sensors, optimal installation is between 14 feet and 7.5 feet above the floor.

c) Moving objects such as fan blades and driven air should be kept out of the coverage pattern.

d) The sensor should be located as far as possible from sources of ultrasonic noise (telephone bells, escaping steam, etc.). Do not aim the sensor toward these items or toward hot or cold spots (radiators, etc.).

e) Other potential sources of nuisance alarms due to "harmonic resonance" are rain on a metal roof, "leaking" compressors, and television or high-fidelity equipment.

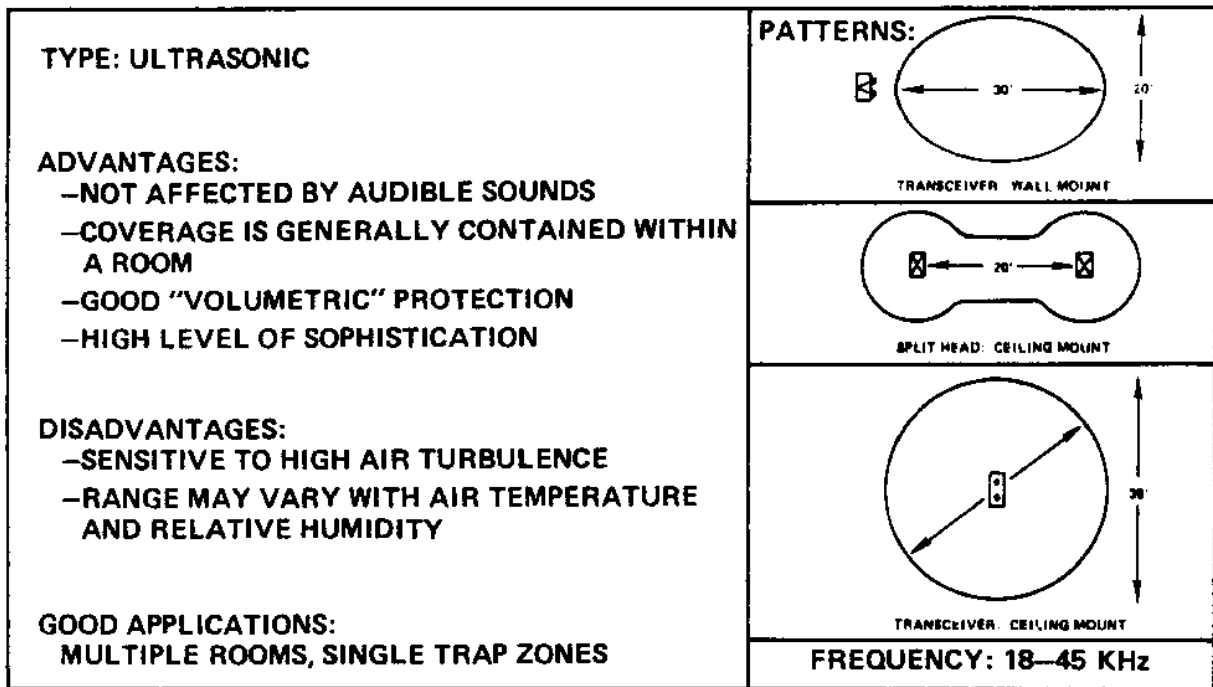


Figure 22
Ultrasonic Sensor Coverages

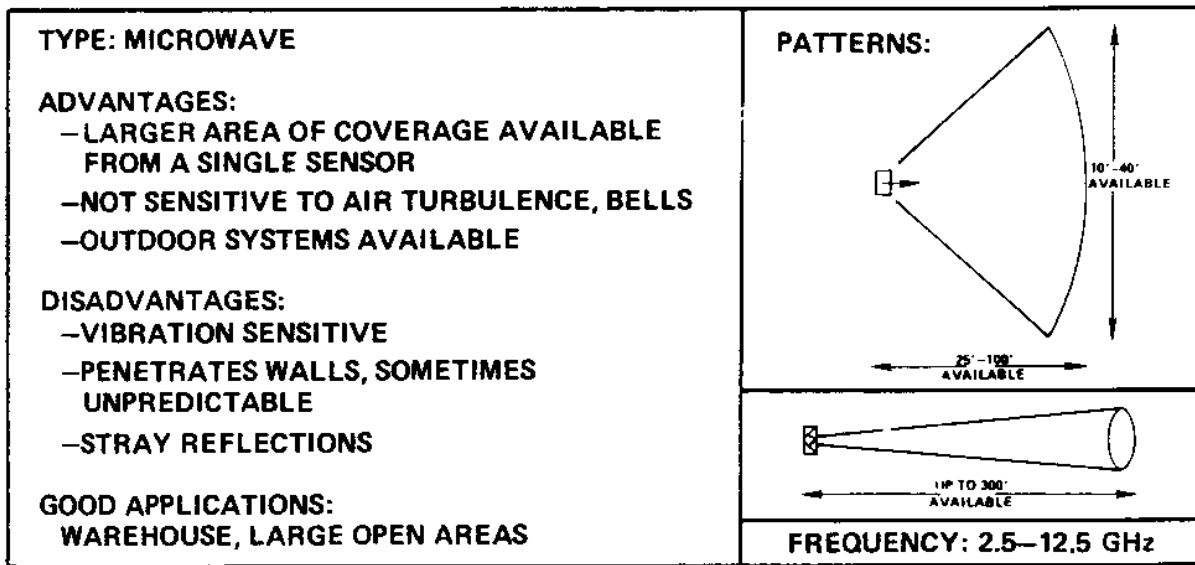


Figure 23
Microwave Sensor Coverages

4.2.3 Microwave Sensors. This sensor consists of a transceiver which transmits and receives a "radar" frequency electronic wave pattern. The sensor electronics will detect an alarm when movement is sensed by causing a change in the received, reflected wave pattern. Most sensors will detect a 3-foot object moving at various speeds. The area of protection can be adjusted by switching antenna, thus widening or narrowing the wave pattern. Pattern examples are depicted in Figure 23. The wave pattern will penetrate glass, masonry walls, and other nonmetallic barriers, while metal objects (even some metal screening) reflect the waves. Penetration of building walls and detection of nuisance stimuli such as vehicular traffic can be a problem. The following considerations for application and installation apply to microwave sensors.

4.2.3.1 Applications. The application for a microwave sensor is similar to an ultrasonic sensor, except that:

a) Microwave sensor energy penetrates most building materials and walls, thus detecting stimuli outside the protected area. Aim of the sensor at an outside wall or window should be avoided.

b) Microwave sensors are not affected by air turbulence.

c) Microwave sensors may interfere with and be interfered by the operation of computers and other electronic equipment.

4.2.3.2 Limitations.

a) Fluorescent lighting is an ionized column of gas which reflects microwaves and can appear as a moving target to this type of sensor. Turning off the lighting when the alarm system is in use can reduce this problem, but also reduces remote visual assessment capabilities.

b) Wind-caused movement of as little as 0.25 inch by large metal objects such as overhead doors can cause nuisance alarms. Positioning the sensor pattern to parallel such nuisance stimuli will reduce nuisance alarms.

c) Potential sources of nuisance alarms such as moving ventilation fan blades can be masked by metal screening.

d) In general, the structure barrier penetration problems and other electronic interference problems limit the use of these sensors in interior DoD applications due to the likelihood of nuisance alarms.

4.2.4 Audio Sensors. These sensors, also called "sound" sensors, consist of one or more microphones connected to an electronic analyser. Ambient environmental noises such as ventilation fans or thunder can be ignored by adjusting the microphones. The analyzer will count "events" such as breaking glass, movement, and conversation, and declare an alarm when an "overload" condition occurs (i.e., when the number of events succeeds a preset number over a period of time). An alarm station operator can listen to the cause of an alarm with an audio sensor's built-in assessment capability. The following considerations for application and installation apply to audio sensors:

a) These sensors are useful to both detect and assess duress situations.

b) Ease of installation is often offset by cost-effectiveness considerations when compared with other types of sensors and visual assessment equipment.

c) Privacy shunts or cut-offs should be specified to preclude normal operations eavesdropping.

d) Alarm station operator overload can easily occur in multiple alarm assessment situations•

4.2.5 Photoelectric Sensors. These sensors, also called "beam" sensors, transmit a beam of visible or invisible light to a receiver. If the beam is interrupted or broken, an alarm is produced. Since visible beams are bypassed easily, only sensors which use invisible light (normally in the infrared spectrum at a frequency of about 1.0 micron) are considered suitable for DoD and USN applications. If the beam is continuous, the receiver may be "captured" by the substitution of another light source, thus permitting bypass. One should use, therefore, only infrared sensors which "pulse" the beam at a certain frequency and make substitution difficult. Modifying the frequency of the pulsed beam will cause an alarm. Generally, infrared transmission is achieved by filtering a visible light source which reduces the effective range of the beam. Pulsing is achieved either by use of propeller blades in front of the light sources or by an oscillator connected to both transmitter and receiver. Because of the mechanical problems which occur with the propeller motor, etc., the latter method is preferred. Also, the pulse modulation is more accurate with the second method, allowing the receiver to discriminate on the basis of phase as well as frequency and provide a higher level of security. Photoelectric sensors can be used outdoors as well for specific applications. The following considerations for applications and installation apply to photoelectric sensors:

a) Alignment is critical. The greater the distance between transmitter and receiver, the more easily misalignment can occur. Mounting on unstable surfaces (e.g., walls which vibrate) also can cause misalignment or nuisance alarms.

b) The use of reflectors is a cost-effective way of extending the sensor coverage. Care must be exercised, however, in the number of reflectors used because this system's detection capability is reduced by each additional reflector introduced.

c) Long, narrow spaces such as corridors are cost-effective applications. Such applications are often called "traps" to back up building perimeter intrusion point sensors.

d) Light beams do not penetrate physical objects and therefore cannot protect masked areas.

e) The vulnerability to bypass can be reduced by employment of multiple beams at various heights.

f) Smoke, steam, or other air particles can degrade performance.

4.2.6 CCTV - Motion Detection. Also called video motion detection, this sensor uses successive images from a closed-circuit television (CCTV) camera to detect motion. A microprocessor digitizes the image signal from a CCTV camera and, at a set interval (1-2 seconds), repeats the process with a second

image from the same camera and performs a comparison for change. Depending upon the sensitivity (larger models can view up to 64,000 individual points on a CCTV picture) and alarm threshold (a selectable preset number of points which must change), if a change is detected, an alarm is declared. The operator sees the reconstituted digital image (versus real time) picture on a monitor. Successive movement produces successive alarm images ("ghosts") on the monitor which remain there, even if the motion stimulus leaves the camera's field of view, until operator reset. Figure 24 depicts the image(s) produced. Models by various manufacturers are available which can handle one, two, four, eight or sixteen cameras. Any CCTV camera can be used, but the sharper the camera image, the better the performance of this sensor. This type of sensor is highly susceptible to nuisance alarms from extraneous motion within the camera field of view. Some models permit "desensitizing" image points which cover nuisance alarm sources, while others provide sensitized squares or rectangles which can be placed over specific areas or objects to be protected. The following considerations for application and installation apply to CCTV motion detection sensors:

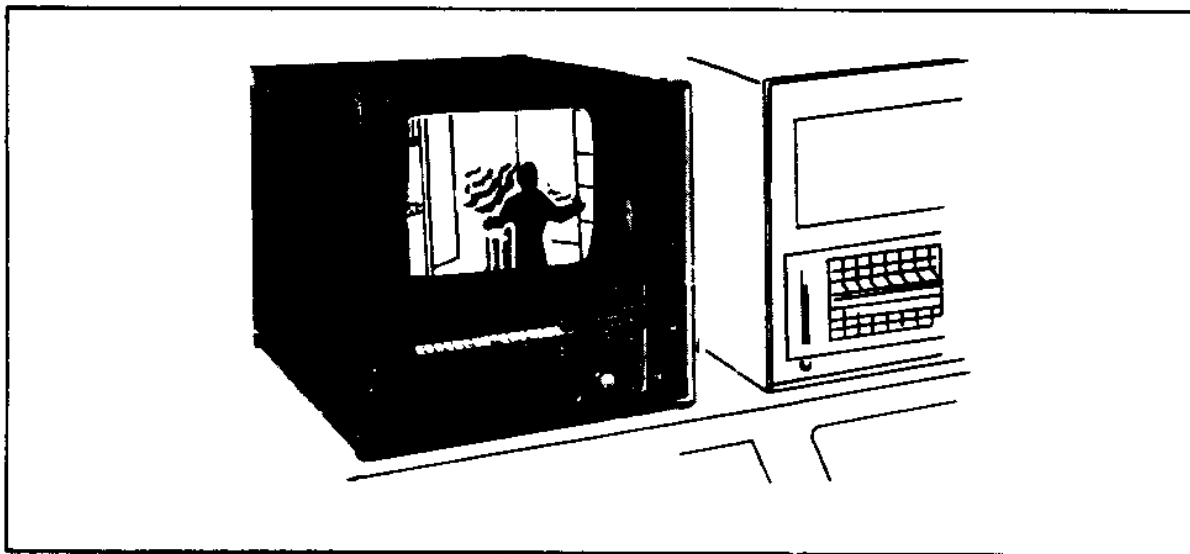


Figure 24
CCTV Motion Detection Sensor Image

- a) Fixed-focus CCTV cameras are most suitable for use with this sensor.
- b) Stable fixed CCTV camera mounting is critical. Any camera movement will be perceived as an alarm state by the sensor.
- c) Cost-effectiveness is a serious consideration compared with the application of conventional volumetric sensors with a CCTV assessment system. In addition, within the sensor type, lower cost CCTV motion detection sensor

models provide only sensitized areas which must be carefully positioned to provide adequate protection. Higher cost models provide sensitized points on the digitized image (the larger the number, the higher the cost) which then must be desensitized individually, as desired, if nuisance stimuli are present. Extensive operator training is required to maximize system performance.

d) Changing lighting shades and reflections from standing water can produce nuisance alarms. The more expensive models have some capability to reject such nuisance stimuli. Careful camera placement, camera field of view selection, and configuration of sensitized image areas are more effective countermeasures against nuisance stimuli.

e) Very large coverage areas require multiple cameras and may require multiple processors if the maximum capacity is exceeded.

f) Visual masking by objects within the camera's field of view will reduce coverage.

g) The most cost-effective application of this sensor to date has been in large open interior areas where no standing water will be present and which have a relatively low activity level.

4.2.7 Interior Sensor Summary. Sensors form the "front line" of the integrated security system. Interior sensors are the last line of defense in providing protection to sensitive resources. Table 4 provides a summary of the strong and weak points of most sensors discussed in this section. Misapplication or "force fitting" of sensor products by vendors can lead to a false sense of security. Table 5 provides, in summary form, application guidelines for sensor selection. Table 6 provides more detail in this area for the most widely used volumetric motion detection sensors. Finally, it must be reemphasized that quality installation is critical. The most well designed sensor subsystem will not work if installed improperly.

4.3 Exterior Fence Sensors. Fence sensors are designed to detect attempts to climb over, lift up, or breach a line of security fencing. Some types detect climbing better than breaching attempts. Others do the reverse. Most fence sensors are designed for installation on an existing fence; others can form a stand-alone barrier themselves. Fence sensors vary in principle of operation and in ease (complexity) of installation. Some characteristics are common to all fence sensors: all require lightning strike protection both for themselves and the fence; all are affected adversely to a greater or lesser degree by wind; all can be bypassed by tunneling under or bridging over the fence; and all will perform best on a well-constructed chain link security fence, designed and installed in accordance with DM-13.01, Physical Security.

Table 4
Interior Sensor Summary

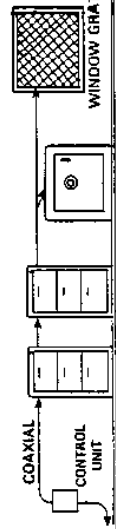
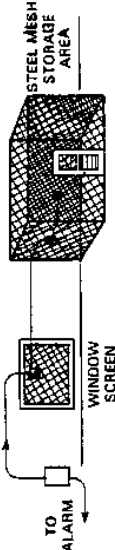
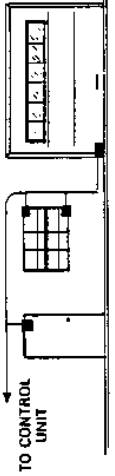

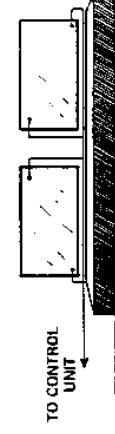

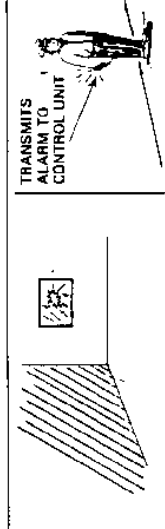

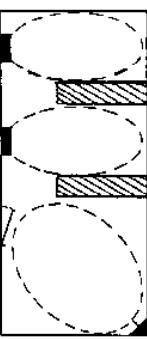
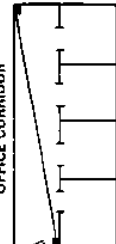

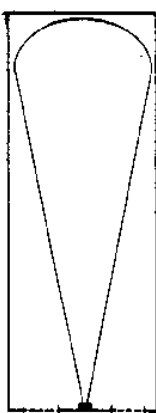
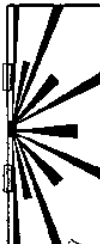

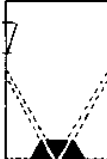

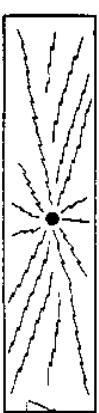
TYPE OF EQUIPMENT	PURPOSE	PRINCIPLE OF OPERATION	COMMON CAUSES OF FALSE ALARMS	GOOD APPLICATIONS	COMPONENT COST RANGE (INSTALLED)	POTENTIAL CONFIGURATIONS
INTERIOR CAPACITANCE PROXIMITY SENSORS	POINT PROTECTION	USED IN CONJUNCTION WITH METAL OBJECTS SUCH AS FILES. THE METAL BECOMES PART OF THE TUNED CIRCUIT AND ANY CHANGE IN THE CAPACITY OF THE TUNED CIRCUIT (E.G., BODY TOUCHING THE OBJECT) CAUSES AN ALARM.	RELATIVELY FREE OF FALSE ALARMS. • PROTECTED ITEMS MUST BE KEPT CLEAN AND MOUNTED OFF THE FLOOR ON BLOCKS.	<ul style="list-style-type: none"> • FILE CABINETS • SAFES • METAL GRATES OR SCREENS • MACHINERY • HARDWARE 	\$200/2200	
VIBRATION SENSORS	POINT PROTECTION	SENSORS ARE MOUNTED WITHIN OR UPON WALLS TO DETECT FORCED ENTRY VIA VIBRATION	<ul style="list-style-type: none"> • VIBRATIONS CAUSED BY LARGE MACHINERY, HVAC EQUIPMENT • THUNDER OR HEAVY WIND 	<ul style="list-style-type: none"> • STORAGE AREAS • VAULT-LIKE ROOMS • CONTROLLED ACCESS AREAS 	\$125 - 160	
DOOR AND WINDOW SENSORS BALANCED MAGNETIC SWITCH	ENTRY/POINT PROTECTION	RECESSED AND SURFACE MOUNTED SENSOR WHICH ESTABLISHES AN ELECTROMAGNETIC CONTACT BETWEEN THE FIXED FRAME AND MOVABLE DOOR OR WINDOW UNIT.	NORMALLY LOW SUSCEPTIBILITY TO FALSE ALARM. POOR INSTALLATION OR MAINTENANCE CAN LEAD TO REDUCED EFFECTIVENESS OR BYPASS.	<ul style="list-style-type: none"> • INTERIOR & EXTERIOR DOORS • WINDOWS • OVERHEAD DOORS 	\$90 - 160	
120 FOIL	ENTRY/POINT PROTECTION	SURFACE MOUNTED ON GLASS. INTRUSION BY BREAKAGE OF GLASS BREAKS CONTACT AND ACTIVATES ALARM.	<ul style="list-style-type: none"> • POOR INSTALLATION • OLD VARNISH BREAKS DOWN • CLEANERS BREAK FOIL • CORROSIVES ON CONNECTORS 	ALL WINDOWS AND GLASS DOORS	\$30 PER STANDARD WINDOW	
120 GLASS BREAKAGE DETECTORS	ENTRY/POINT PROTECTION	SURFACE MOUNTED ON GLASS. USES ULTRASONIC SIGNAL GENERATED BY GLASS BREAKAGE TO SIGNAL AN ALARM.	SOME PRODUCTS CAN BE ACTIVATED BY WINDOW VIBRATION.	ALL WINDOWS AND GLASS DOORS	\$45 EACH	
SWITCH MATS	POINT PROTECTION	PRESSURE SENSITIVE FLOOR MATS ACTIVATED BY INTRUDER'S BODY WEIGHT.	LOW FALSE ALARM POTENTIAL. MOISTURE COULD CAUSE SHORT CIRCUIT.	<ul style="list-style-type: none"> • IN FRONT OF SAFES, FILES AND CASH REGISTERS • IN DOORWAYS AND STAIRWELLS • UNDER WINDOWS • UNDER CARPETING IN EXECUTIVE OR OTHER OFFICES 	\$125	
WIRELESS DURESS ALARMS	POINT PROTECTION	WIRELESS ALARM ACTIVATING SYSTEMS ARE USED TO SEND ALARM SIGNALS OVER THE AIR TO A REMOTE CENTRAL RECEIVER.	ACCIDENTAL ACTIVATION BY THE USER. WALLS AND OTHER BARRIERS WILL REDUCE EFFECTIVE RANGE.	<ul style="list-style-type: none"> • GUARDS ON PATROL WITHOUT COMMUNICATIONS • AS A MONEY CLIP IN RETAIL OR CASH DEPOSITORIES • LOCAL COURIERS 	\$140	

Table 4
Interior Sensor Summary (Continued)

TYPE OF EQUIPMENT	PURPOSE	PRINCIPLE OF OPERATION	COMMON CAUSES OF FALSE ALARMS	GOOD APPLICATIONS	COMPONENT COST RANGE (INSTALLED)	POTENTIAL CONFIGURATIONS
ULTRASONIC SENSORS	SPACE PROTECTION	EMITS MAUDIBLE SOUND WAVES THAT ARE SENSED BY A RECEIVER. INTRUDER ALTERS WAVE PATTERN ACTIVATING AN ALARM.	AREAS CONTAINING: • ROTATING OR MOVING MACHINERY • ESCAPING AIR OR STEAM • LARGE GLASS WINDOWS OR THIN WALLS THAT CAN VIBRATE • RADIO TRANSMITTERS • MAGNETIC FIELDS FROM MOTORS OR GENERATORS • FLUTTERING DRAPES	ROOMS WITH UNBROKEN LINE OF SIGHT. LARGE OBJECTS SUCH AS STACKS OR FURNITURE CAN CREATE SHADED AREAS ON THE SIDE AWAY FROM THE TRANSDUCER. MULTIPLE UNITS TO BE USED IN THESE APPLICATIONS.	\$150 - 275	 
PHOTO ELECTRIC BEAM (ACTIVE INFRARED SENSORS)	SPACE PROTECTION	DIRECTS INVISIBLE INFRARED LIGHT BEAM AT A RECEIVER. ANY INTERRUPTION OF THE BEAM RESULTS IN AN ALARM.	• ALIGNMENT BETWEEN TRANSMITTER AND RECEIVER CRITICAL. FREQUENT CHECKS REQUIRED. • HEAVY DUST. HEADLIGHTS	• DOORWAYS • LOADING DOCKS • AISLES • CORRIDORS • ALONG INVENTORY STACKS • A LINE OF SIGHT SENSOR USING A PENCIL ZONE OF PROTECTION.	\$185 - 189	 
MICROWAVE SENSORS	SPACE PROTECTION	TRANSMITS AN ELECTRO-MAGNETIC FIELD INTO THE AREA TO BE PROTECTED. INTRUDER MOTION ACTIVATES ALARM.	AREAS CONTAINING: • SMALL OPENINGS WHICH CAN ALLOW ESCAPE OF MICROWAVE ENERGY TO OUTSIDE AREAS • FLUORESCENT LIGHTS • HEAVY MACHINERY • WALL VIBRATION • THIN WALLS OR GLASS • RADIATED OR CONDUCTED ELECTRO-MAGNETIC RADIATION	LONG CORRIDORS, AISLES OR TOTALLY ENCLOSED AREAS OR AREAS IN WHICH SENSOR CAN BE DIRECTED AWAY FROM WINDOWS AND THIN WALLS. IN WELL CONSTRUCTED BUILDINGS, GOOD FOR LARGE SPACE PROTECTION, NOT AFFECTED BY AIR CURRENTS OR TEMPERATURE DIFFERENTIAL.	\$225 - 450	
PASSIVE INFRARED SENSORS	SPACE PROTECTION	COMBINATION OF HEAT GENERATED BY A BODY PLUS MOTION OF THE BODY ACTIVATES THE SENSOR.	• OBJECTS IN A ROOM HEATED BY SUNLIGHT THROUGH WINDOWS • SPACE HEATERS • RODENTS AND ANIMALS HIGH RESISTANCE TO COMMON FALSE ALARMS.	ROOMS OR AREAS WITH HIGH AIR TURBULENCE. ALL INTERIOR SPACES. SENSOR SHOULD BE MOUNTED SO THAT DIRECT SUNLIGHT IS NOT IN THE SENSOR'S DIRECT FIELD OF VIEW.	\$180 - 240	 
SONIC (AUDIO) SENSORS - ACTIVE -	SPACE PROTECTION	FILLS THE AREA TO BE PROTECTED WITH SOUND WAVES. DISRUPTION OF THESE WAVES BY INTRUDER ACTIVATES ALARM.	MAY BE ACTIVATED BY EXTRANEOUS SOUNDS FROM OUTSIDE THE PROTECTED AREA. OBJECTS WITHIN A ROOM WHICH CAN MOVE SUCH AS FANS OR EQUIPMENT. SOUNDWAVES CAN BE DISTURBED TO PERSONS IN ADJACENT AREAS.	INTERIOR SPACES WHERE STAY-BEHINDS ARE A THREAT OR IN WHICH ITEMS IN THE AREA MAY BE IN DIFFERENT LOCATIONS FROM DAY-TO-DAY. SUCH AS WAREHOUSES OR SHIPPING AREAS.	\$200 - 250	 
AUDIO/REMOTE LISTEN-IN PASSIVE	SPACE PROTECTION	USES LEASED TELEPHONE LINE AND MICROPHONE TO PROVIDE REMOTE LISTENING CAPABILITY TO DETECT INTRUDER MOVEMENT.	EXTRANEOUS NOISE. MISTAKENLY CLASSIFIED AS AN INTRUSION. (PASSING VEHICLES, MACHINERY, NOISE IN ADJACENT AREAS, ETC.)	PROVIDES A MEANS TO VERIFY OTHER INTRUSION SYSTEMS PRIOR TO RESPONSE.	\$350 PER UNIT	

Environmental and Other Factors Affecting Sensor Usage	(Circle one)	Effect on Sensor			Recommendations and Notes
		Ultrasonics	Microwave	Passive I/R	
1. If the area to be protected is enclosed by thin walls or contains windows, will there be movement near the outside of this area?	Yes No	None	Major	None	Avoid using a microwave sensor unless it can be aimed away from thin walls, glass, etc., which can pass an amount of microwave energy.
2. Will protection pattern see sun, moving headlamps, or other sources of infrared energy passing through windows?	Yes No	None	None	Major	Avoid using a passive I/R sensor unless pattern can be positioned to avoid rapidly changing levels of infrared energy.
3. Does area to be protected contain HVAC ducts?	Yes No	None	Moderate	None	Ducts can channel microwave energy to other areas. If using a microwave sensor, aim it away from duct openings.
4. Will two or more sensors of the same type be used to protect a common area?	Yes No	None	None (See note)	None	Note: Adjacent units must operate on different frequencies.
5. Does area to be protected contain fluorescent or neon lights that will be on during protection-on period?	Yes No	None	Major	None	Microwave sensor, if used, must be aimed away from any fluorescent or neon light within 20 ft.
6. Are incandescent lamps that are cycled on and off during protection-on period be included in the protection pattern?	Yes No	None	None	Major	If considering passive I/R sensor, make a trial installation and, if necessary, redirect protection pattern away from incandescent lamps.
7. Must protection pattern be projected from a ceiling?	Yes No	None, but only for ceiling heights up to 15 ft.	Major	Major	Only <u>ultrasonic</u> sensors can be used on a ceiling, but height is limited to 15 ft. At greater ceiling heights, either (1) use rigid ceiling brackets to suspend sensor to maintain 15 ft. limitation, or (2) in large open areas try using a microwave sensor mounted high on a wall and aimed downward.
8. Is the overall structure of flimsy construction (corrugated metal, thin plywood, etc.)?	Yes No	Minor	Major	Minor	<u>Do not use a microwave sensor!</u> Where considerable structural movement can be expected, use a rigid mounting surface for ultrasonic or passive infrared sensor.
9. Will protection pattern include large metal objects or wall surfaces?	Yes No	Minor	Major	Minor (major if metal is highly polished).	1. Use ultrasonic sensor. 2. Use passive I/R sensor.
10. Are there any nearby installations?	Yes No	Minor	Major when radar is close & sensor is aimed at it.	Minor	Avoid using a microwave sensor.

Environmental and Other Factors Affecting Sensor Usage	(Circle One)	Effect on Sensor			Recommendations and Notes
		Ultrasonics	Microwave	Passive I/R	
11. Will protection pattern include heaters, radiators, air-conditioners, etc.?	Yes No	Moderate	None	Major, when rapid changes in air temperature are involved.	1. Use ultrasonic sensor, but aim it away from sources of air turbulence desirable to have heaters, etc., turned off during protection-on period). 2. Use microwave sensor.
12. Will area to be protected be subjected to ultrasonic noise, e.g., bells or hissing sounds.	Yes No	Moderate, can cause problems in severe cases	None	None	1. Try muffling noise source and use an ultrasonic sensor. 2. Use a microwave sensor. 3. Use passive infrared sensor.
13. Will protection pattern include drapes, carpets, racks of clothing, etc.?	Yes No	Moderate, reduction in range	None	Minor	1. Use ultrasonic sensor if some reduction in range can be tolerated. 2. Use a microwave sensor.
14. Is the area subject to changes in temperature and humidity?	Yes No	Moderate	None	Major	1. Use an ultrasonic sensor unless changes in temperature and humidity are severe. 2. Use a microwave sensor.
15. Is there water noise from faulty valves in the area to be protected?	Yes No	Moderate, can be a problem.	None	None	1. If noise is substantial, try correcting faulty valves and use an ultrasonic sensor. 2. Use a microwave sensor. 3. Use a passive I/R sensor.
16. Will protection pattern see moving machinery, fan blades, etc.?	Yes No	Major	Major	Minor	1. Have machinery, fans, etc. turned off during protection-on period. 2. Use careful placement of ultrasonic sensor. 3. Use passive infrared sensor.
17. Will drafts or other types of air movement pass through protection pattern?	Yes No	Major	None	None, unless rapid temperature changes are involved.	1. If protection pattern can be aimed away from air movement, or if air movement can be stopped during protection-on period, use an ultrasonic sensor. 2. Use a microwave sensor. 3. Use a passive I/R sensor.
18. Will protection pattern see overhead doors that can be rattled by wind?	Yes No	Major	Major	Moderate.	1. If protection pattern can be aimed away from such doors, use an ultrasonic sensor. 2. Use a passive I/R sensor.
19. Are there hanging signs, calendar pages, etc. which can be moved by air currents during protection-on period?	Yes No	Major	Major	Moderate, can be a problem.	1. Use ultrasonic sensor, but aim pattern away from objects that can move, or remove such objects. 2. Use passive infrared sensor.

Environmental and Other Factors Affecting Sensor Usage	(Circle one)	Effect on Sensor			Recommendations and Notes
		Ultrasonics	Microwave	Passive I/R	
20. Are there adjacent railroad tracks that will be used during protection-on period?	Yes No	Major	Minor	Minor	A trial installation is required if using an ultrasonic sensor.
21. Can small animals (or birds) enter protection pattern?	Yes No	Major	Major	Major (particularly rodents)	Install a physical barrier; prevent intrusion by animals or birds.
22. Does area to be protected contain a corrosive atmosphere?	Yes No	Major	Major	Major	None of these sensors can be used.
Approximate installer cost per square foot of coverage:	_____	(3d)	(4d)	(6d)	_____

The following matrix is intended as a guide only and does not represent absolutes but suggests areas for consideration.

ENVIRONMENTAL AND OTHER VARIABLES	ULTRASONIC	PASSIVE INFRARED	MICROWAVE
Vibration	No problem with balanced processing, some problem with unbalanced	Very few problems	Can be a major problem
Effect of temperature change on range	A little	A lot	None
Effect of humidity change on range	Some	None	None
Reflection of area of coverage by large metal objects	Very little	None, unless metal is highly polished	Can be a major problem
Reduction of range by drapes, carpets	Some	None	None
Sensitivity to movement of overhead doors	Needs careful placement	Very few problems	Can be a major problem
Sensitivity to small animals	Problem if animals close	Problem if animals close but can be aimed so beams are well above floor	Problem if animals close
Water movement in plastic storm drain pipes	No problem	No problem	Can be problem if very close
Water noise from faulty valves	Can be a problem Very rare	No problem	No problem
Movement through thin walls or glass	No problem	No problem	Needs careful placement
Drafts, air movement	Needs careful placement	No problem	No problem
Sun, moving headlights, through windows	No problem	Needs careful placement	No problem
Ultrasonic noise	Bells, hissing, some inaudible noises can cause problems	No problem	No problem
Heaters	Problem only in extreme cases	Needs careful placement	No problem
Moving machinery, fan blades	Needs careful placement	Very little problem	Needs careful placement
Radio interference, AC line transients	Can be problem in severe cases	Can be problem in severe cases	Can be problem in severe cases
"Piping" of detection field to unexpected areas by A/C ducting	No problem	No problem	Occasional problem where beam is directed at duct outlet
Radar interference	Very few problems	Very few problems	Can be problem when radar is close and sensor pointed at it
Cost per square ft.-large open areas	In between	Most expensive	Least expensive
Cost per square ft.-divided areas/multiple rooms	Least expensive	Most expensive	In between
Range adjustment required	Yes	No	Yes
Current consumption (size of battery required for extended standby power)	In between	Smallest	Largest
Interference between two or more sensors	Must be crystal controlled and/or synchronized	No problem	Must be different frequencies

An important consideration is the establishment of a clear zone around the fence for alarm assessment. Since most fence sensors consist of multisensing devices strung together at varying intervals, or one continuous sensing device, the DoD has established a nominal standard of 100 meters length for fence sensor alarm zone reporting and display. Fence corner zones and gates normally have shorter lengths, but 100 meters is the normal standard and most fence sensor electronics are configured to that length. The paragraphs below discuss the presently available commercial fence sensors as well as a short discussion of other barrier protection applications. A key point to remember is that because fence sensors are subject to intruder bypass and to the adverse effects of an outdoor environment, they should never be the only type of sensor employed to provide effective intrusion detection. Properly employed, fence sensors can provide an important contribution to the overall effectiveness of an integrated IDS.

4.3.1 Electromechanical Fence Sensors. This type of sensor is similar in operation to the vibration or shock sensors used for building perimeter penetration detection as discussed in paragraph titled "Vibration/Ultrasonic" of this section. Normally each sensor is installed on the fence posts at 10-foot intervals in a conduit housing. Figure 25 depicts such an installation. The sensors, which contain a simple switch mechanism, are connected in series to form a sensor zone. The vibrations associated with attempts to breach or climb the fence are detected by the sensors which provide the switch closure or opening to tell the electronic control unit for the sensor zone that an alarm has occurred. The control unit generally senses (counts) switch closures over a preset time period and, if the criteria is met, declares an alarm. Vibrations associated with wind-induced fence vibrations can also be counted and, in the better quality models, discriminated to minimize nuisance alarms to some degree. The more advanced versions of this type of sensors use multiple masses within the individual sensors, both of which must move to declare an alarm and which also permit better sensitivity adjustment to reduce nuisance alarms. The following considerations for application and installation apply to mechanical fence sensors.

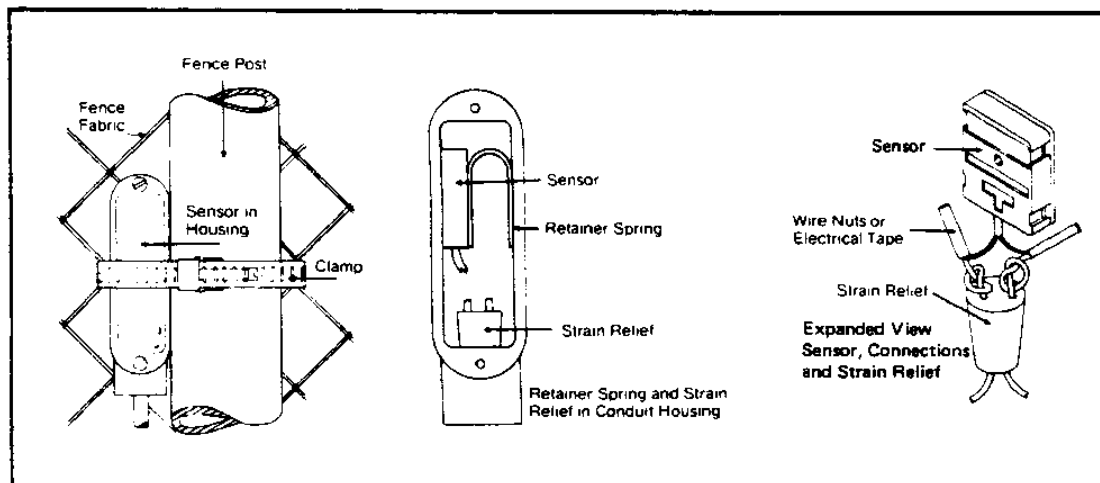


Figure 25
Electromechanical Fence Sensor

a) To provide optimal performance, the fence must be of good quality construction with tight tension maintained. This type of sensor requires frequent fence maintenance.

b) Signs, barbed concertina tape, and other items attached to the fence are a source of nuisance alarms for this sensor.

c) To provide tamper resistance and minimize environmental wear and tear, the cable connecting the sensors should be installed in conduit.

d) This fence sensor is generally rated by DoD test agencies to provide 0.90 probability of detection at 90 percent confidence level if of modern, good quality manufacture with a single or multiple mass switch instead of a simple mercury or other tilt switch, and with electronic processing.

e) Line supervision and tamper protection on the cable connecting the sensors as well as on the processing electronics should be specified.

f) This sensor should be mounted on the inside (protected area side) of the fence.

g) This sensor requires extensive electronic adjustment to minimize nuisance alarms due to wind and is generally rendered inoperable in wind speeds in excess of 25 mph, depending upon direction.

4.3.2 Strain Sensitive Cable. This sensor consists of an electret cable attached to the fence fabric and a signal processor mounted on the fence fabric. Zone lengths can be up to 1000 feet, but are normally the DoD standard length of 100 meters. A signal produced in response to deformation in the transducer cable caused by movement or cutting of the fence or fabric is transmitted to the processor. If the frequency and time duration of the disturbance satisfy predetermined criteria, an alarm is generated. The processor provides for adjustment in amplifier gain, the number of disturbances required to generate an alarm, and alarm time. The sensor is tamper self-protecting. Figure 26 depicts the cable composition in detail, as well as a type installation. The cable is connected normally with plastic ties to the fence. The following considerations for application and installation apply for the strain sensitive cable.

a) This type of sensor also has an inherent audio assessment capability. The electronics to provide an alarm station operator with that capability is normally an extra cost option.

b) Different colored cable is available. The use of black colored cable should be avoided in hot, sunny areas due to expansion/contraction of

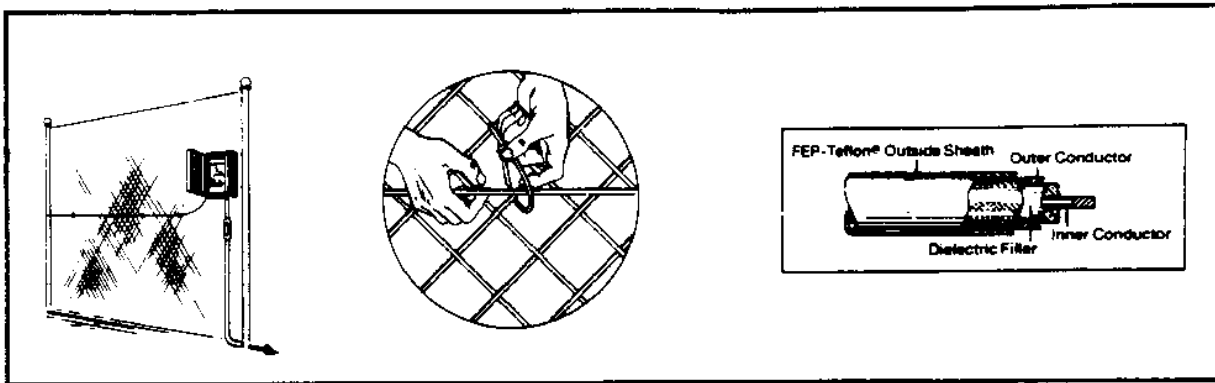


Figure 26
Strain Sensitive Cable Sensor

the cable caused by sun loading on the cable.

c) A taut fence is not required for effective performance of this sensor. The attendant reduced cost in fence maintenance may be a significant consideration.

d) This sensor can function with degraded performance level in winds up to 35 knots.

e) This sensor has been performance rated by DoD test agencies to provide a probability of detection of 0.90 at a 90 percent confidence level.

f) Sensor alarm outputs are from the electronics processor, not directly from the cable.

g) This sensor may be mounted on the inside of the fence or interlaced through the fabric.

h) Gate continuity units are available for strain sensitive cable sensors to provide continuous protection.

4.3.3 Electrostatic Field Fence Sensors. Also called E-field sensors, this type of sensor can be used as a stand-alone sensor for perimeter intrusion detection or can be attached to a fence. The sensor consists of one

or more field or transmitter wires, two or more sensor (receiver) wires, and a combination crystal-controlled E-field generator, amplifier, and sensor signal processor for each sensor zone. A minimum of one transmitter and two sensor wires are required to adequately cover a standard 8.5-foot high chain link security fence upon which it is mounted. Four or more wire configurations are common. An electrostatic field transmitted by the transmitter wire is received by the sensor wires. Then, any disturbances in the field are detected and an alarm declared. Adjustments to the alarm threshold are possible. The wires are kept under tension to maintain field stability. The configuration usually resembles an inverted "T." Figure 27 depicts an electrostatic field sensor configuration. The following considerations for application and installation apply to the electrostatic field fence sensor:

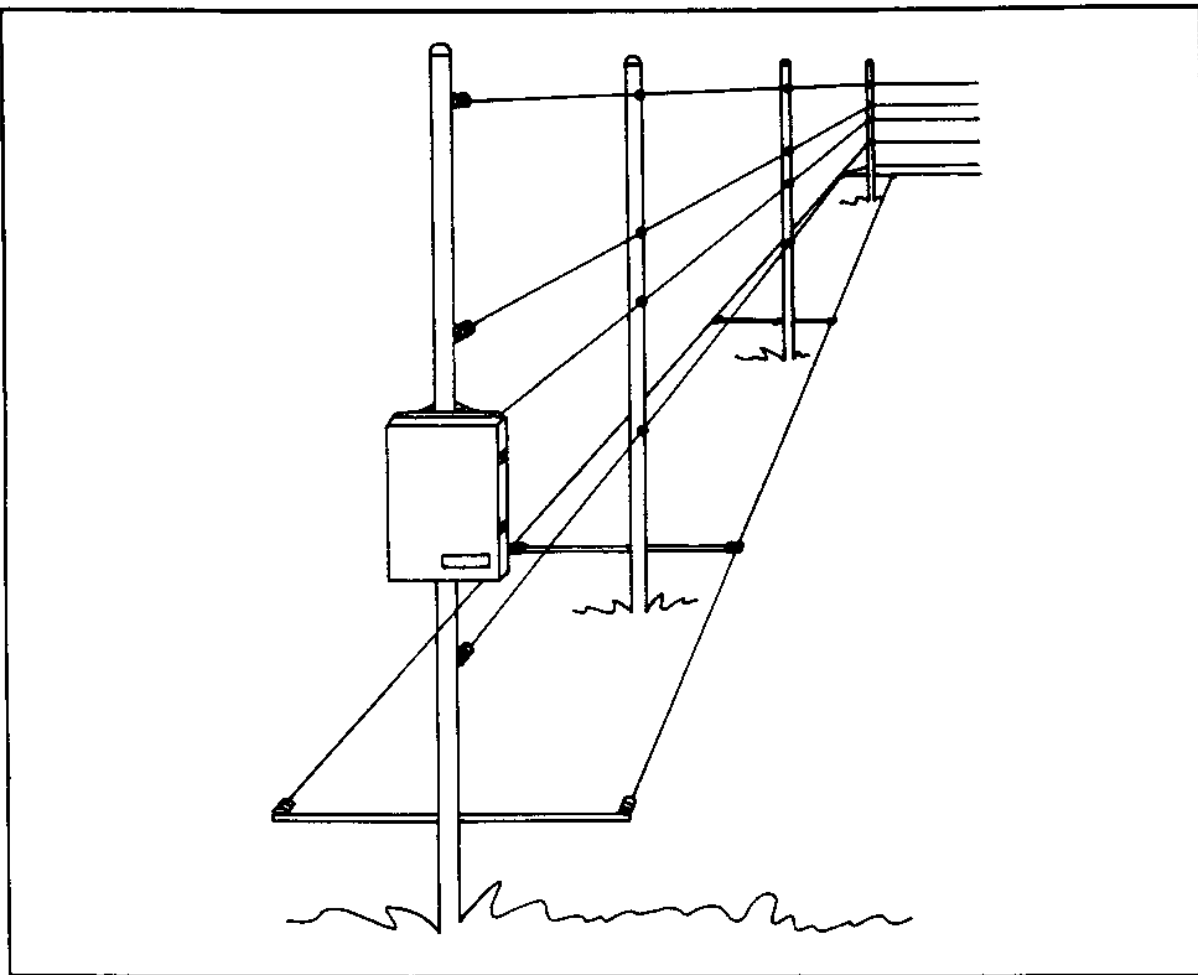


Figure 27
Electrostatic Field Sensor

a) Even with sensitivity adjusted to reject leaves, etc., a tight, well maintained quality fence is required, as any significant disturbance in the electrostatic field can cause an alarm. Since the field extends above the fence, outrigger barbed wire/tape must also be taut.

b) Performance in deep snow or with ice or frost coating is degraded.

c) Wire tension maintenance devices have not met performance standards in the past.

d) Metal fatigue of transmitter (field) and sensor (receiver) wires and required repair should be considered.

e) Chain link fence fabric limits the electrostatic field. Mounting on the inside of the fence reduces nuisance alarms, since no field change is sensed until the fence fabric is deformed by either climbing or breaching. Mounting on the outside of the fence will detect an intruder's approach (as well as other nuisance stimuli). Mounting is generally only effective on the inner fence of a dual fence perimeter. Stand-alone mounting enlarges the detection zone width, but increases cost significantly.

f) Minimizing nuisance alarms requires removing all vegetation within a 4-to 6-foot radius of the electrostatic field. Continuous and extensive maintenance is a must to assure optimal sensor performance. The cost of this maintenance may be a consideration, as may be the aesthetic requirement for a denuded clear zone.

g) Gates and other fence openings should be protected by the sensors.

h) Application in areas with large bird populations should be avoided since the sensor attracts birds as a roost, causing nuisance alarms.

i) Wind affects the sensor by causing deformation of the field or fence fabric, and debris may penetrate the field resulting in nuisance alarms.

4.3.4 Taut Wire Sensors. This type of sensor may be used as a stand-alone sensor and barrier, or may be attached to the outside of an existing fence. This sensor consists of a series of horizontal wires under tension with 6-inch vertical separation, mounted through ring eyes or slider clips on the exterior of the fence posts covering the entire fence area. These wires are normally barbed to increase barrier effectiveness. Tension is maintained by wire springs at both ends of the sensor zone. These wires are mechanically clamped to a vertical wire, called a sensor wire, attached within a special sensor post in the center of the sensor zone. This wire is connected to transducers which convert mechanical motion to electronic signals. The

processor analyzes these signals to determine if any alarm state exists. The sensor is stable in quiescent or windy conditions and not affected by environmental influences when equal on both sides of the vertical sensor wire. Any vertical displacement of one of the horizontal wires by climbing or breaking attempts are mechanically converted to a horizontal displacement of the sensor wire and converted and analyzed by the sensor processor as an alarm signal. The processor will provide automatic equilibrium adjustment to return to a quiescent state after an alarm event has been assessed and reset. For example, the cutting of one horizontal wire will cause an alarm, and if not replaced, the system will automatically adjust to the new condition upon reset. This sensor has been defeated only by highly sophisticated intruders after repeated attempts. The following considerations for application and installation apply to the taut wire sensor:

a) Figure 28 depicts various types of taut wire sensor applications. Note that barbed tape or plain wire may be used instead of barbed wire.

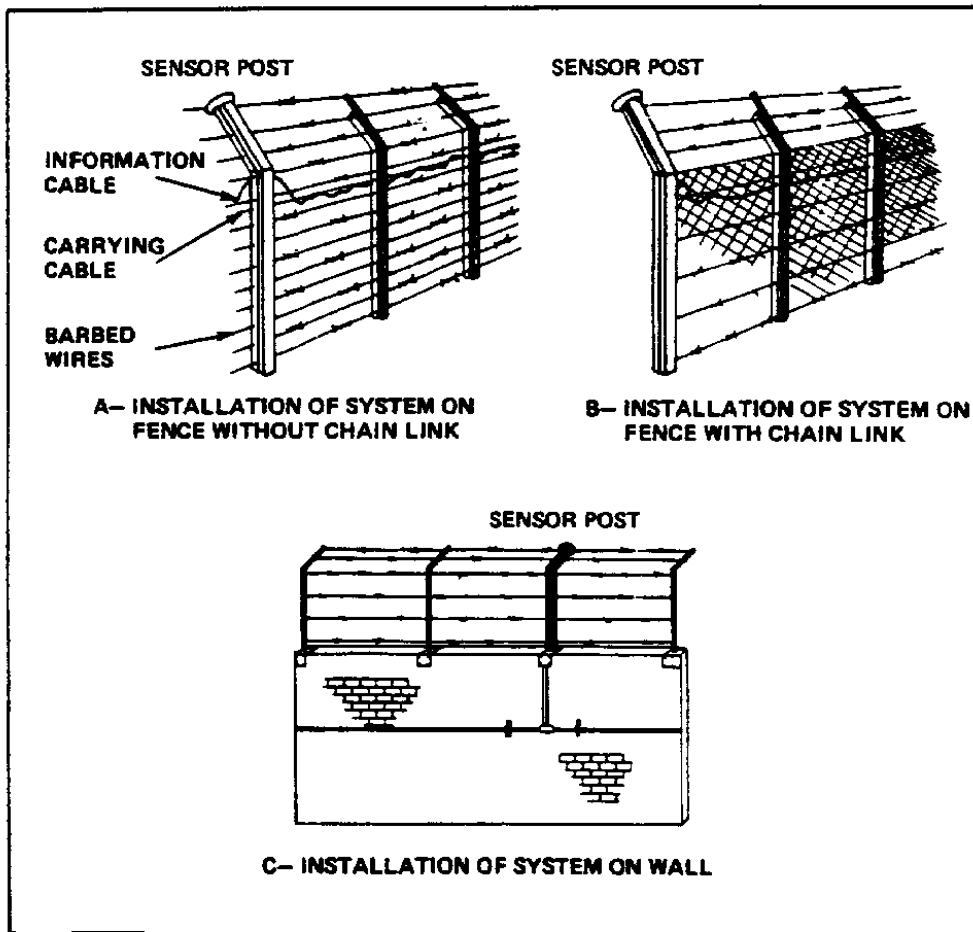


Figure 28
Taut Wire Fence Sensor Applications

b) As presently manufactured, this sensor's maximum zone length is 60 meters.

c) Cost of installation of this sensor type is much higher than other fence sensors.

d) This sensor is effective on non-chain link fences, while other sensors with the same number of units have reduced effectiveness.

e) Consider the extensive maintenance required of this sensor.

f) The taut wire sensor has been rated by DoD testing agencies to provide a probability of detection in excess of 0.95 at a confidence level of 95 percent. However, keep in mind that any fence sensor is subject to defeat or bypass and therefore should not be the only sensor used to protect a facility.

4.3.5 Balanced Magnetic Gate Switch (BMS). Many fence sensors do not provide for continuity of detection capability through fence gates. Termination of zones are required on either side of the gate opening. To provide continuity of protection by detecting gate openings, BMS models are available for application to gates. They are suitable for outdoor use and allow a wider opening gap before alarming to compensate for the "play" that generally exists between gate halves or the space between gate and ground surface. They interface readily with the overall IDS. If not recessed, BMS should have tamper protection. Other application and installation considerations are the same as for other BMSs as discussed in paragraph titled "Balanced Magnetic Switches."

4.3.6 Barrier Protection. Fence sensors may be applied successfully to protect walls and other similar barriers. Mechanical, electromechanical fence sensors, and electrostatic field sensors may be used to detect breach attempts. Both taut wire sensors and electrostatic field sensors may be applied to detect climb over attempts. Capacitance proximity sensors using special outrigger wires can also be used for fence tops as well as other barriers. Pulsed infrared (photoelectric beam) sensors may also be used to detect both breaching and climbover attempts. Other exterior sensors which are not addressed in this manual may also be used. A successful barrier protection design is only limited by the competence and imagination of the designer. As with any other application, quality installation is a must. Consideration should also be given to a test of a sensor zone configuration to confirm design prior to final installation.

4.3.7 Exterior Fence Sensor Summary. Table 7 depicts a summary of various exterior fence sensors' application considerations based upon data compiled in the Department of Energy's (DOE) Sandia National Laboratory (SNL) Intrusion Detection Handbook. The sensors listed have been in use for several years at various DOE and public utility facilities. Their capabilities and limitations are well documented. Fence sensors can form a valuable portion of an IDS provided that the security system designer recognizes their capabilities and properly applies this information in the design criteria.

Table 7
Summary of Exterior Fence Sensors

APPLICATION	OPERATING PRINCIPLE	AVAILABILITY	DETECTION					CONDITIONS FOR UNRELIABLE DETECTION	TYPICAL DEFEAT METHODS	MAJOR CAUSES OF FALSE ALARMS										
			NONMAGNETIC	WALK, RUN & CRAWL TUNNEL	CLIMB FENCE	CUT FENCE	HIGH WINDS			HEAVY RAIN	HEAVY SNOW	HEAVY FOG	BIRDS	SMALL ANIMALS	LARGE ANIMALS	THUNDER & LIGHTNING	ELECTRICAL TRANSIENTS	RFI		
FENCE ASSOCIATED	STRAIN SENSITIVE	PRODUCTION	●			●		HIGH WIND	LADDER OR SHORT TUNNEL	●							●	●	●	
	MECH TILT SWITCH	PRODUCTION	●			●		MODERATE WIND	LADDER OR SHORT TUNNEL	●							●			
	TAUT-WIRE	PRODUCTION	●			●	●	STAND-ALONE SENSOR	LADDER OR SHORT TUNNEL								●			
	E-FIELD	PRODUCTION	●	●		●	●	HEAVY PRECIPITATION	TILT OR HIGH BRIDGE					●	●	●	●	●	●	●

4.4 Duress Alarms. Duress alarms are used by operational and security personnel to signal a duress situation. General application considerations include high reliability, the ability for surreptitious activation, and annunciation remotely from the area where the duress situation is occurring. The security system designer should consider also that duress alarms signal life-threatening situations and call for special reaction(s) by responding security forces. This section will discuss various types of duress alarms as well as other approaches to duress situation indication.

4.4.1 Hardwire Duress Alarms. Also called "holdup alarms," this type of sensor consists of a mechanical switch normally positioned near the person who will activate it. Banks and Credit Union tellers and other cashier-type personnel who handle large amounts of cash and deal with the (military) public are obvious personnel who may need these devices. Other applications are central alarm station guards, building and facility alarm station guards, police desk sergeants, and fixed post watchstanders. Most devices are designed to be foot-activated and require lifting up rather than pressing down to preclude accidental activation. Covers also protect against accidental activation. Many types and configurations are available. High reliability and simple design will assure ease of use and proper functioning under crisis conditions. Always consider incorporating these devices in security system design. Make provisions in the security system design for their use and upgrade plans for thorough training and detailed procedures as well for actions required by security personnel.

4.4.2 Radio Frequency Duress Alarms. The present mature state-of-the-art devices resemble paging beepers. They consist of a device about the size of a pack of cigarettes and are carried inconspicuously on the belt or in a pocket. Positive activation of an external switch normally activates this device. This causes a radio frequency signal to be sent to a control unit in the local area for further transmission to a central alarm station for action by security personnel. Some belt-mounted units also incorporate a tilt switch with a timer that automatically activates the alarm signal if the bearer is not standing or sitting after a preset period of time. This unit may initially have a high nuisance alarm rate due to user adaptation. However, it has been documented and the security system designer should plan for an initial high nuisance alarm rate with the introduction of any portable duress system. Fixed duress devices have been in use for a very long time; user confidence tends to be high from the start. Portable devices are relatively new; thus, users should expect and plan for some confidence-building trials. Obvious applications include any roving guard personnel, key personnel in the chain of command, and other key personnel who are not at fixed operating posts. The critical design consideration is range of transmitter to relay station or control unit. A large range safety margin (50 percent minimum) should be allowed for use in case an abduction attempt delays immediate activation. Considerations of fixed duress alarm system applications also apply.

4.4.3 Other Approaches to Duress Notification. The sensors discussed above may not always provide the required application solutions for the security system designer. Consider especially that "procedure-oriented" duress notification approaches require detailed documentation, thorough training, and frequent changes of codes to preclude compromise. These other approaches to duress notification are:

a) Incorporation into an automated access control system by use of a special personal identification number (PIN), changing the PIN by one number, or omitting or adding a digit.

b) A special voice code.

c) A special action which would seem out of place to operational personnel but appear perfectly normal to an "outsider."

d) Limited only by the imagination of the security system designer.

Section 5: BASIC AUTOMATED ACCESS CONTROL SYSTEMS

5.1 Importance of Access Control to Security Operations. Simply defined, access control is a process which serves to permit or deny entry, thus regulating the flow of personnel and/or material into a protected area. The criteria for approving access also involves verification of an authorization to enter the protected area or use a restricted device. The criteria can be verified through one or more of the elements of security: personnel, equipment, and procedures. The proportion of use of these three elements to authorize access involves analysis both of the specific threat(s) to the protected area or object and the requirements of operational procedures to assure mission accomplishment. The systems discussed in this section refer to basic electronic and electromechanical devices which are commercially available and designed to provide automated unlocking of a portal without human intervention by use of previously authorized credentials.

5.1.1 Increased Use of Automated Access Control in Security Operations. The growth of application of automated access control systems in high security environments has been due probably more to potential cost tradeoffs than any other criterion. Once the basic need for reliable entry authorization/verification was established, prior methods tended to concentrate upon the manned entrance: the guard who would manage a time-consuming sign-in/sign-out or badge exchange procedure. Internal procedures then relied upon maintenance of an effective key and lock system with all of its inherent vulnerabilities. The use of microprocessor technology and recent advances in coded credentials have led to the ability of lower cost systems to electronically control access and perform a host of ancillary functions from a single security control point. The employee credential, the badge, is now increasingly the access authorization means, and the central processor is providing alarm display, control, and related total system integration functions. With sufficient intelligence, these systems can perform highly sophisticated authorization and reporting functions with the simple insertion of the coded credential and pay for themselves with reduced or redirected manpower costs.

5.1.2 Electronic Access Control Requires Effective Planning. It takes careful and effective analysis to design and implement an electronic access control system. At between \$1000 and \$2000 per controlled door, costs can escalate rapidly and overtake the capabilities of many system configurations. The number of routine and nonroutine (periodic) enrollees in the system, card credentials type, the number of doors to be controlled, required/desired system functions, and ancillary duties of the systems such as alarm reporting and display, all require careful thought and planning prior to specification.

5.2 Components of Automated Access Control Systems. Automated access control systems, as considered here, are systems which permit a machine to grant or deny access based upon prior approval of authorization criteria encoded into a badge credential. This approval authorization sequence is information which must be communicated to the equipment in forms acceptable to the electronics. This information provides the criteria for the access and

egress. On the following page, Figure 29 presents a simple block diagram of an access control system. The elements noted in the figure are common to all automated access systems and discussed in detail in the following paragraphs.

5.2.1 Coded Badge. Commonly, the access approval relates to a number or other distinctive information encoded within a badge or token. These systems often utilize a credit card-sized (3 1/4 by 2 inches) coded identification credential. The card material is plastic, vinyl, or polyester composition depending upon environmental characteristics at the facility and if photo identification images are to be incorporated.

5.2.1.1 Badge Technologies by Type. The coded badge technologies indicated in Section 2, Figure 8 represent those commercially available. These technologies are characterized by the information storage which identifies the distinctive card holder. Coded badge technologies are susceptible to decoding and duplication given appropriate time, technical expertise, and funding. The relative susceptibility to decoding and duplication is noted below as a guide which may be of significant value if an activity requires more secure credentials. Except as noted below, factory manufacture/coding does not preclude local assembly to add photographs and printing.

a) Magnetic Stripe. This technology is characterized by a stripe of magnetic material capable of containing encoded information. The stripe data are encoded in Aiken Code, a two-frequency, coherent phase recording. The standards for this encoding relate to the relative position of information on the stripe. The Track 1 standard is a 210 bits per inch (BPI) or 79 characters maximum. Track 2 encoding is a 75 BPI or 40 characters maximum. The more common encoding is the Track 2 type as used and standardized by the American Bankers Association. The categories of magnetic stripe cards are also broken down into the two encoding energies used with this media. The low energy (300 oersted) is more common than the high energy (4000 oersted) type. Obviously, the high energy types are less susceptible to accidental erasure. Encoders are available to permit a using activity to produce encoded badges on site, thus saving cost by buying blank or preprinted stock.

b) Magnetic Spot. This badge refers to a plastic laminated card which incorporates a sheet of ferromagnetic material with spots strongly and permanently magnetized on the core material. These spots may be polarized, and they number between 20 and 100 in a media more stable than magnetic stripe due to the high energy encoding. Caution should be exercised when placing this card with bank cards or magnetic tape/stripe media due to the others' susceptibility to erasure. The magnetic spot badge can be decoded and duplicated without great difficulty. The badge is manufacturer encoded but may be assembled on site for photograph or custom printing additions.

c) Optical. Credentials which have rows of spots or lines that change under specific illumination are optically encoded. The general optically encoded badge contains spots or lines that absorb, transmit, or reflect infrared or another specific light spectrum. The change constitutes the unique code which is facility and card specific. This badge type is

easily decoded, but more difficult to duplicate. The encoding is manufacturer processed, but custom printing must account for specific ink colors which are critical to the read technique.

d) Hollerith. Rectangular punched holes similar to a computer keypunch card are the means of storing information on the Hollerith card. The amount of information which can be stored is quite limited. The storage space available is even less where a photograph or other printing are also required on the card. This card is extremely vulnerable to copying with inexpensive tools.

e) Electric Circuit. This card is essentially a plug-in printed circuit which can present a limited number of unique codes. The unique codes are values of continuity or electrical pathways on the card. The card is decoded and simulated easily with inexpensive, unsophisticated tools. This card is encoded in the factory but may be assembled by users.

f) Metallic Strip. This badge consists of a matrix of metal (usually copper) strips which are laminated to a badge core. A moderate amount of information can be encoded by the presence or absence of strips. The card is easily simulated. This card is factory encoded but may be assembled locally to add custom artwork and photographic images.

g) Wiegand Effect. The Wiegand badge contains a series of small parallel wires laminated within the card. These wires are manufactured from ferromagnetic materials which produce a sharp change in magnetic flux when exposed to a slowly changing magnetic field. The wires' placement above and below a critical centerline determines the specific information in binary code. This technology is factory-encoded and therefore impossible to erase and difficult to alter or duplicate.

h) Proximity. Proximity badges are essentially tuned antennas laminated within the core of a card. A weak radio signal is spectrum generated by the card reader and is attenuated and reflected to the reader as specific information. The information on the badge can be decoded, but the card is difficult to alter or duplicate.

i) Capacitance. The capacitance badge contains an array of capacitor plates which are connected (or not) to a specific pattern. This pattern is the limited information code. Although affected by wetness, this factory-encoded badge is difficult to read, alter, or duplicate.

j) Active Electronic. This miniature transmitter contains the individual code which is sent when energized by the reader. The media is characterized by the very limited amount of information storage. This card can be decoded with instruments, although it is moderately difficult to duplicate.

5.2.1.2 Secondary Credentials. As noted previously, all card access badges are susceptible to alteration, decoding, and duplication. The degree to which the technology is resistive to these threats is very important to the integrity of the security system. Controls placed on badge stock, enrollment of cards into the system, and changes in authorization should be well audited. Secondary verification systems, which require either a code to be entered on a keypad or physical data sampling in addition to a valid card read are usually required for entry into very sensitive areas. The second verification is to minimize the adverse effects associated with unreported lost or stolen cards. Examples of secondary verifications are physical characteristic photographic image matchup to files of personnel, personal identification number (PIN), hand geometry, fingerprints, handwriting, speech, weight, and other biometric systems. Secondary systems, with the exception of biometric systems, are less secure than coded credentials. This is due to the easily read identification media and the wide latitude to accommodate variations due to environment, stress, and other data entry errors which may deny access to authorized users. A personal identification number is the most commonly used secondary verification system because of the relative ease in obtaining an accurate specific data entry and the immunity of this data to environmental influences.

5.2.1.3 General. Most card access systems utilize either 2 1/8 by 3 3/8 inch or 2 3/8 by 3 1/4 inch credit card-sized credentials. Some technologies permit much larger cards, which may be used as identification, to be worn and read easily using larger photographs and printing. Characteristics of specific card technologies provide a mixture of pro and con attributes which should be balanced to best effect for the activity or facility. The ability to decode, alter, or duplicate the badge, the sensitivity of the coding to accidental alteration or erasure, the physical attributes of size, thickness, stiffness and durability, the amount of coded information, and requirements of manufacturer or user encoding can be either assets or liabilities depending upon the activity or facility viewpoint. Each of these features affect cost.

5.2.2 Badge Reader. Information which has been encoded in the various media represented by the badge technologies must be decoded or read, then transmitted to a processor which grants or denies access based upon a comparison of the encoded information with authorization files. The encoded information is usually set up in at least two segments. The first segment, a facility specific code group, is used to exclude those information sets which do not belong to the facility. The decision to pass the information to the processor enrollment files is done at the controller. The reader devices depend upon the types of media presented. The second set of information is specific to the card holder and usually not duplicated within the system. Some systems using only facility code in the event of communication breakdown are termed degraded mode operations systems and are not recommended for higher security facilities.

5.2.2.1 Magnetic Stripe. Magnetic stripe features the largest information storage media capacity. Readers are available for indoor and outdoor application. The low-energy readers require close tolerance or spring loaded and gimbel mounted readheads to compensate for the faint signal presence. The

high-energy reader permits the readhead to have a coating which resists wear. The reader is generally the insertion type that reads upon withdrawal, which provides for a steadier motion upon insertion. The high-energy type reader is often the swipe-through type due to the ability to read the stronger signals quickly. The swipe reader is more appropriate to turnstyle applications since a high throughput can be maintained (approximately 12 per minute nominal).

5.2.2.2 Optical Reader. The optical reader senses either a transparency or reflectance of light as individual identification codes. Photosensitive cells read the relative transmissivity of the light and translate this into the identification. The reader type is usually insertion. Although durable and low in cost, the badge requires some care to avoid dirt and inks which inhibit accurate reads.

5.2.2.3 Hollerith Reader. The Hollerith reader operates similarly to the optical reader. The punched holes permit light passage through the card to the photosensitive array. Although durable, this card requires prohibition of bend, fold, spindle, and mutilate.

5.2.2.4 Electric Circuit Reader. The electric circuit card reader contains an edge connector into which the card is literally plugged. The reader determines the current passage through the circuit as the identification code. The reader technology is spoofed easily by using electronic instruments if a valid card can be examined and tested. The card is generally much thicker than a credit card and thus unsuitable to wallet or pocket storage. The card is also particularly susceptible to stresses associated with bending or flexing.

5.2.2.5 Metallic Strip Reader. Electric brushes which make contact to copper sheets incorporated in the card are the essential components of this reader. The electrical continuity between the copper sheets and brush points produce the binary code combination. This reader system is susceptible to corrosion and other faults which inhibit good electrical contact to the metallic strips. Outdoor applications are vulnerable to moisture.

5.2.2.6 Wiegand Reader. The Wiegand reader decodes the card information by producing a slowly changing magnetic field that affects the specially treated ferromagnetic wires. When the wires pass by the readhead, a series of sharp pulses are created which represent binary information. Since there are no moving parts in the reader, it is not affected by moisture, humidity, or strong magnetic fields. Care should be taken to protect the associated data wiring from sources of electromagnetic interference or shared cable and conduit of fluorescent lighting and electromechanical devices, particularly electric strikes. The swipe through reader style is effective in indoor and outdoor applications. There is also an insertion reader available for recessed wall mounting and "key" style credentials. Custom card designs are inhibited due to the precise alignment of the code strip required to operate

the system. Attempts to alter the code strip should result in irreparable damage to the strip and inoperability of the card.

5.2.2.7 Proximity Reader. The proximity reader generates weak radio signals, some of which are absorbed and reflected by the card. The receiver sends the resonated information along to the controller for code comparison and access authorization. The reader attributes permit mounting behind materials which pass radio frequencies -- glass, wood, plaster, and plastic -- if the 4- to 6-inch proximity of card to reader can be attained. This feature can enhance aesthetics but may inhibit service and relocation of the device. The reader should be protected from vandalism and physical attack.

5.2.2.8 Capacitance Reader. The capacitance reader passes weak electrical current to the capacitor plates imbedded within the card. The absorption of the electrical energy at specific points on the capacitor array is the coded information. The influences which inhibit electrical continuity from the reader to the card must be avoided. The card is subject to poor contact problems.

5.2.2.9 Active Electronic Reader. In this technology the reader supplies current to the transmitter contained within the card. Further, this insertion reader enhances and transmits the signal to the controller electronics. This technology as well as others is being improved, particularly in the area of circuit miniaturization. The durability of cards, too, has been improved.

5.2.2.10 General. Since the insertion, swipe, receiver, and proximity reader types are all located on the edge of the protected perimeter, they are all affected by an environment which is difficult to control. Direct physical attack upon the reader is not uncommon. Compromise of connection wires and application of foreign voltages, and insertion of foreign objects and substances (including but not limited to: debris, sticks, coins, chewing gum, "Superglue," ice, liquids, or chemicals) are vulnerabilities of varying degrees for all readers. The above effects can be diminished by sheltering (including sun shading) of the reader to mitigate the adverse environment. The best protection from the human attack is afforded by surveillance and early detection of attacks. In all cases, no system should be implemented which permits unauthorized access by the manipulation of electronics outside the protected perimeter.

5.2.3 Electric Door Locks. Locking hardware that is compatible with automated access control systems are electric strikes, electric bolts, and electromagnetic locks. Each of these devices is available with one of two features termed "fail-safe" and "fail-secure" configured in either alternating or direct current in a range of 6 to 240 volts. The design of an automated access control system must consider such variables which are related to portal use and application of local and national fire and electrical codes.

5.2.3.1 Electric Strikes. The electric strike is the most commonly used electric lock. This device provides a depression or channel that fits the

mechanical bolt with a common knobset hardware or vertical push bar device. The keeper channel catches or releases the bolt, depending upon the lock status. The strike is either surface or recess mounted on the door frame. Considerations for device choice include composition of the door frame, size and shape of latch bolt, and the holding force or potential for abuse of the door lock. Recommendations for locking hardware with access control systems usually require the heavy-duty type of locks. Options for this device include latch bolt monitor, indicating whether the bolt is extended into the strike; lock cam monitor, indicating whether or not the strike is in a locked position; a combination of both features and additional switches, indicating if door is shut and locked, and an interlock feature to permit only one door in a series to be unlocked at a time as in man-trap or energy conservation foyer applications.

5.2.3.2 Electric Bolts. Electric bolts provide positive locking by pushing a solenoid-operated rod into a hole in the door edge. This device requires critical alignment between the bolt and the locking strike. This device is used generally for interior door application, since the electric bolt may not meet certain safety code regulations for egress doors. In U.S. Navy applications, electric bolts shall have a minimum throw of one inch.

5.2.3.3 Electromagnetic Lock. The electromagnetic lock consists of a power magnet and a steel plate. The magnet is mounted to the door frame in alignment with the steel plate in order to provide a strong or hardened area to apply magnetic force. This device is inherently fail safe since power is interrupted to unlock, and fail-secure types maintain power with backup battery supply. Minor variations in door alignment and problems associated with door settling and warping can be addressed by use of this device. Pairs of doors can be secured by a single device if both swing in the same direction (outswing or inswing).

5.2.3.4 Fail-Safe/Fail-Secure. There are two operations of an electric door lock if power is removed. These two operations are termed Fail-Safe and Fail-Secure as follows: if the power fails, the lock becomes either SAFE for access/egress or SECURE - locked. Considerations in application of these two types is often due to fire code, electrical code, or activity regulations which consider that in the event of an emergency - fire or catastrophe - the human seeking to exit is not capable of rapid thought and logical reasoning and thus requires a simple, usually entirely mechanical, means of exit. The spirit of this requirement is to assure that speedy exit is accomplished without having to read directions or depend upon electrical or electromechanical devices which may fail due to the emergency condition.

5.2.4 Remote (Control) Units. The remote control unit is that component of the access control system which translates communications and performs interface tasks between credential readers, electric door locks, and the central control unit. This intermediate device is usually subject to distance constraints and is often located to accommodate line length from readers and central control unit. The functions of a controller include interpretation of coded information to the central control unit. If the facility code criteria

is met, a relay is operated to energize or open an electric lock and close the electric lock after the proper elapsed time. The controller also may supply conditioned power to the reader. Some system configurations utilize controller electronics within the reader assembly. Caution is advised when using this type of system. Most system requirements indicate a need to have all decision-making electronics within the protected perimeter to avoid any compromise that may result in defeat of the system.

5.2.5 Central Control Unit. The central control unit refers to the electronic devices which process information regarding the automated access control.

5.2.5.1 Enrollment Console. The enrollment console is the device used to initiate the authorization status of an encoded badge. This device can be a keyboard, badge reader, or video display terminal. Information entry regarding badge authorization can include badge number, employee number, name, address, telephone, motor vehicle registration, status, issue date, return date, authorization center, and portal restrictions by time zones, entry/exit status, and trace. Also included may be a commentary section which is often utilized for emergency call lists and other safety-related information. The enrollment display usually consists of a fill-in-the-blanks or input directions that permit a large volume of authorizations to be processed as a clerical task. Changes of high authorization levels are generally password or software protected to prevent unauthorized use of the system. It is recommended to have passive software protection on all system functions.

5.2.5.2 Central Processor. Decisions based upon information files entered at the enrollment console are conducted by a central processing unit in collaboration with memory and operating systems. This device communicates with remote controllers and checks the encoded information input against the existing files; it then approves access based upon the filed authorizations. The central processor also creates a historical file of attempted accesses and the manipulations of the existing files. This history may be recorded either electronically in computer storage media or printed on paper for later permanent review. The information files in computer storage media are available for statistical and other manipulative processing and reporting in a variety of report formats. Power loss will often affect the system memory; backup power systems should be considered to maintain integrity.

5.2.5.3 Printer. The printer is an output device which provides a hard copy record of activities reported by the central processor. Considerations of printers with systems include sufficient speed and appropriate buffer to avoid information omissions from overload by the much faster system electronics. The print speed is often controlled by the quality of type fonts, cost, and data transmission technique. Security systems do not generally require letter quality printing; therefore, faster printing can be accomplished with fewer cost constraints. Care and security of printer output must be seriously considered, particularly if the only historical reporting is based upon real time activity printing. This type of record will realize a great importance in the event of security breaches or other need to develop an

audit trail. Minimum requirements of printed reports are date, time, activity, location, and action taken. The using activity should consider the worst case projections of report needs and cost justify those needs based upon the vulnerability of the activity or sensitivity of the mission. Maximum flexibility can be attained with a computer storage media historic system. This system enhances system efficiency by permitting exceptions to routine and timed reporting controls in contrast to recording real time occurrences of alarms and other events with no differentiation between them.

5.3 Automated Access Control System Functions. Computer based systems permit flexibility in controls and remove the mundane, repetitive tasks from the guard's duties. Previous justifications for access approvals are consistently checked against the access requests and recorded appropriately. This automation permits greater efficiency of guard personnel while reducing the number of personnel required and improving security to the facility.

5.3.1 Access Authorization/Verification and Reporting. Approval for personnel to enter a specific portal, based upon the system parameters, will require advance justification to the facility authority and subsequent approval for system enrollment. Approval or denial of access requires the electronic check of limitations associated with the encoded credential at the time of each access request. The machine operates without prejudice on a repeatable basis. Approval authorization is reduced to a routine task that requires human intervention only in the event of exceptions. The system will note and report, of course, exceptions and operator-initiated actions. Human failures or errors are controlled, while a commercial industry system standard of 2 seconds maximum for routine access approval is maintained.

5.3.2 Area Authorization. The access authorization can be as general as system wide approval or as specific as individual portal restrictions. The files associated with authorizations should consider the appropriate classification of a portal that comprises a perimeter barrier to security or restricted areas (see OPNAVINST 5530.14). The portal should be assigned the classification of the restricted area and allow access only to persons permitted within the area. The activity authority having security jurisdiction should consider authorizations based upon need-to-know principles, since such access normally constitutes an uncontrolled admittance to the area. The guidelines developed by various directives can be assigned with little modification on most commercial systems.

5.3.3 Time Zoning. Further definition of access authorization can be based upon a criteria of time. Access may be approved only if the individual is authorized to enter a portal during an appropriate time period. Time codes may also be designated in a way which precludes all access during a time zone assigned to a portal. Thus, either individuals or areas may be excluded from access based upon the definition of time periods. Applications of the feature may be beneficial if regular working hours or closed hours are established at the facility. Nonduty hours security operations at the facility can then rely upon routine patrols and the functions of the intrusion detection system

without compromise associated with turning off portions or all of the intrusion detection system. The criteria here are time of day, day of week, and 8-day calendar (includes holidays scheduled as the eighth day).

5.3.4 Fail Safe/Fail Soft. If the communication lines between the controller and the central processor are severed, then the default parameters within the system are exercised. Two schemes are available to address this problem. The first, "fail safe," prohibits access even if the criteria of correct facility code is met. The fail soft scheme is also referred to as degraded mode. Access is granted normally upon correct facility code entry. A caution must be observed; few systems in the degraded mode record access information for later transmission to the computer when the communication line is restored.

5.3.5 Occupant Listing. These programs are software functions which process entry information and permit the report by area of occupants, maximum number or load of personnel, or enforcement of the "two-man" rule. Specific reader configurations and entry and exit readers must be used in conjunction with anti-passback on tailgate or piggyback prevention controls. The controls must be utilized to assure accurate representation of the data gathered in conjunction with access authorizations. The computer compiles useful lists only if all entries and exits are indicated. The safety aspects and the "two-man" security aspect can be controlled with this manipulation of information. Evacuation plans and evacuation assurance can be realized by this feature.

5.3.6 Anti-Passback. Exclusion of access or egress approval in the event of two successive "in" or "out" access requests is anti-passback. This exclusion prohibits the unauthorized use of a single card by two persons until an exit read is accomplished. This avoids the event where one individual obtains access and, while inside, "passes back" the access credential. Tailgating or piggyback is a fault in automated access control systems where two persons gain access with one card at the same time. A single authorized card is used and approved, but two persons enter during the door unlock time window. This problem is critical in sensitive facilities, particularly if duress situations are a threat. The problem can be addressed by an interlocking man-trap with visual guard assessment equipment, the use of closed-circuit television assessment in addition to access control at portals, or the lesser effective beam break and personnel counting devices with appropriate alarm/delay features. The best solution, though, would be the use of a rotary gate (turn-style) connected to the access control system.

5.3.7 Security Enhancement. The standard features of the automated access control system provide enhancement of security operations, particularly where the equipment outperforms the human. This creates a more secure environment since the human element is permitted to perform in the area where greater efficiencies are achieved. Definitions of whom is permitted access based upon the criteria of area, portal, time zone, holiday schedule, loading, two-man rule areas, and the subsequent recording of the information relative to utilization can be essential to the mission of security. The automation of

electronic alarm processing within the same control center provides a single source of information regarding the facility or activity security. The other software enhancements of automated guard tours and patrols, fire system monitoring, security trace, data encryption, and centralized control/reporting can improve the versatility of the system. The capabilities of the system to call up electronic pages of probable requirements to address detected events with specific details, telephone numbers, and prioritized sequences reduce further the margin for human error by reducing the requirements for human judgment.

5.4 Modularity - Building in Expansion and Growth. As a general rule of thumb, the installed system should consider an expansion capability of 25 percent with minimum hardware and software additions. The best method to accomplish this is to have a basic system which will permit additions of equipment to meet expansion without obsolescence of existing hardware. The step additions in hardware permit maximum configurations to the point of outgrowing the central processor and then requiring additional processors or different processors. State-of-the-art special purpose processing equipment is designed to be implemented in building blocks, with logical breaks, in order to meet the differentiations of applicable individualized usages. Modules which are specific task oriented and software modifications often provide the required capabilities most cost-effectively.

5.5 Considerations for Application and Installation. Variables which impact the choice of access control equipment manufacturer include: total number of anticipated cardholder population, throughput requirements, type and volume of data base available with the system, types of reports required by the user, ease of system use, and vulnerability of the system to attack, vandalism, and compromise. An accurate vulnerability and requirements analysis will provide vital information which will impact this choice of equipment technology, manufacturer, and systems integrator. Since the selected group of responsive vendors will, in most cases, provide for "turn-key" installations, a maintenance contract for hardware and software is highly recommended. The proposal for maintenance should be examined as part of the life cycle cost of the system. The general guidelines in the following table and the commentary related to coded badge and reader types are the primary requirement criteria for system implementation (see Table 8).

Table 8
Card Access Guidelines

<ul style="list-style-type: none">○ THE SYSTEM CHOSEN SHOULD BE ABLE TO ACCOMMODATE THE REQUIRED NUMBER OF BADGES, BADGE READERS, AND ACCESS LEVELS.○ DISTANCE REQUIREMENTS BETWEEN THE LOCATION OF THE BADGE READERS AND THE CONTROL PROCESSOR SHOULD BE OBSERVED.○ THE SYSTEM CHOSEN SHOULD PROVIDE TAMPER ALARMS TO DETECT TAMPERING WITH THE ELECTRICAL EQUIPMENT.○ THE SYSTEM CHOSEN SHOULD BE ABLE TO DETECT TAMPERING WITH THE LINES THAT CONNECT THE BADGE READERS TO THE CENTRAL PROCESSOR.○ A REASONABLE AND ADEQUATE MAINTENANCE CONTRACT SHOULD BE NEGOTIATED, STATING REPAIR RESPONSE TIME.○ COMPETENT ELECTRONIC TECHNICIANS MUST BE AVAILABLE FOR REPAIR AND MAINTENANCE OF THESE COMPLEX ELECTRONICS SYSTEMS.○ ASSURANCE MUST BE PROVIDED BY THE MANUFACTURER AS TO AVAILABILITY OF REPAIR PARTS AND PRESTOCKAGE OF KEY PARTS, ON-SITE, BASED ON FREQUENCY OF REPAIR.○ THE CENTRAL PROCESSING UNIT AND OTHER CONTROLLING ELECTRONICS (INCLUDING ELECTRIC STRIKES) SHOULD HAVE BATTERY BACKUP TO ENSURE PROPER SYSTEM OPERATION IN THE EVENT OF POWER FAILURE.○ BADGE CONSTRUCTION MATERIALS SHOULD BE SUITABLE TO THE ENVIRONMENT TO PERMIT A LIFE OF 5 YEARS UNDER DAILY USE. SOME CARD MATERIALS CAN BECOME BROKEN OR WARPED UNDER COLD AND HEAT CONDITIONS.
--

Section 6: REMOTE ALARM ASSESSMENT

6.1 The Role of CCTV in Security Operations. Presently, the primary means of remote alarm assessment is closed-circuit television (CCTV). (Other remote assessment means such as audio assessment are in use, but are used primarily as inherent additional features of particular sensor systems. These have been briefly addressed in Section 4. They will not be discussed further in this manual because of their extremely limited use in USN applications. Other means such as binoculars, night vision devices, etc. are beyond the scope of this DM.) CCTV's value in increasing the efficiency and effectiveness of security personnel is well recognized. It has been proven as a cost-effective alternative to human on-the-spot assessment, and has a demonstrated return value by facilitating security upgrades without the normally attendant and expensive manpower authorization increases. This section will discuss CCTV so that the security system designer will be able to apply this element of the security system properly to the overall security system design. The discussions will be limited to black and white CCTV components since, at the present time, color components have not been proven cost-effective for most security applications.

6.1.1 Near Real Time Alarm Assessment. This is the most common use of CCTV and operates on the concept of allowing a remotely located human (guard, watchstander, etc.) to assess one or several alarmed sensor zone(s) in near real time. The term "near real time" is used to denote the difference between the direct visual assessment in "real time" possible when a guard is stationed directly at an alarming sensor location and the time delay associated with remote alarm assessment using CCTV. The resultant difference in time is comprised of the time it takes for the sensor alarm signal to be processed, for the appropriate CCTV camera to be selected, and for the resultant scene to be displayed to the remotely located alarm station monitor. With modern solid state electronics, this time delay varies from one to a few seconds, depending upon system design. Emerging technologies, such as digitized video frame storage, will enable a remotely located alarm station monitor to also view the scene of an alarm sensor zone at the instant of initial sensor alarm. At the present, to minimize video data display delay time and thereby minimize the time until viewing of the alarmed sensor zone scene after the alarm event, two techniques may be used. The first is to have the entire video system display all sensor zones for the alarm monitor continuously. This is not recommended because it induces boredom and fatigue and is expensive due to the number of CCTV monitors required. The second and preferred technique is to have the system active continuously, but to display no video data to the alarm monitor until an alarm event occurs. This eliminates electronic warmup time delay as did the first technique but also assures that alarmed sensor zones receive immediate attention when an alarm event occurs. The use of a video switcher with this second technique reduces the number of monitors required for display of data for the entire system. (The use of video switchers and operator control options is covered further in paragraph titled "Options for Enhanced Capabilities.") Near real time alarm assessment by CCTV facilitates effective alarm response direction in an economical manner.

6.1.2 Alarm Response Direction. One of the most important functions of the alarm station monitor is to direct appropriate response to an alarm situation. CCTV eliminates the need to rely upon verbal reports from fixed manned observation posts. It enables alarm station personnel to tailor the response to the viewed alarm cause. Procedures should require that all actual intrusion alarms and all alarms should be responded to, especially those for which no cause can be immediately determined. An example of a tailored response would be that for an alarm zone which will not reset, it may be appropriate to send maintenance personnel with the responding security forces. In short, CCTV, when used with prudent operational procedures, can increase security system effectiveness in responding to an intrusion alarm.

6.1.3 Directed Surveillance. CCTV may be used for surveillance of protected areas or spaces as directed by Navy regulations or by local directives or procedures. Pan and tilt camera mounting platforms are used normally because they enable more cost-effective coverage of a large area than with multiple fixed cameras. Caution in use should be considered; attempts to use surveillance cameras for alarm assessment may result, causing misassessment or no assessment of an alarm event. Personal privacy areas and areas where classified materials are used are usually off-limit areas for surveillance by remote devices. It should also be remembered that surveillance is not a substitute for IDS coverage. Human factors studies have verified that alarm station personnel can only focus their attention on a surveillance monitor for a short period of time before becoming inattentive. Normally, remote surveillance is required of several areas which also results in inattention because of distraction by activity on other monitors. In summary, CCTV surveillance can be an effective supplement to the security system but should be used prudently lest it become a perceived panacea when only the illusion of effective security is achieved.

6.1.4 Event Recording. Recording is a valuable tool to enable reconstruction of alarm events, analysis of nuisance/false alarms by maintenance personnel, and for reviewing by alarm monitor personnel for assessment in the case of multiple alarm scenarios. CCTV systems accomplish these objectives through the use of video tape recorders (VTRs) to record video data as required. Video tape recordings have been accepted as evidence in both civil and federal court and in courts martial provided that a custodial "chain" for the recording can be documented (as for any other key evidence). Further discussion on VTR types and application is contained in the paragraph entitled "Options for Enhanced Capabilities." Event recording can assure coverage of alarm events when alarm monitor personnel are not present and can assist command personnel in reviewing significant events. While this capability can be expensive relative to other assessment subsystem components, it has often proved cost-effective in many Navy applications when compared with human-intensive solutions.

6.1.5 Access Monitoring. CCTV is sometimes used for remote monitoring of access (entry/exit) control points. This application is suitable for general monitoring of access flow and central activity monitoring. However, it has proven unreliable in assuring positive identification of individuals, such as picture badge-face comparison, especially under high throughput requirement

situations (e.g., shift changes). It is sometimes employed as an access verification device at relatively small areas with low personnel portal throughputs (e.g., small command posts) as a supplement to other automated access verification means. It is especially useful when direct surveillance of the access portal area is not possible by security personnel. The use of CCTV as a primary access control means is not recommended.

6.2 Components of Basic Closed-Circuit Systems. Figure 30 depicts an example of the components of a CCTV system. The components include the lens and camera which "see" the scene, the cable or other transmission media and associated components over which video data is transmitted, and the monitor and associated components upon which the video data is displayed. While Figure 30 depicts the basic components of a CCTV system, most systems are much more complex. Cable and other video transmission media will be discussed in Section 7. The remainder of this section will discuss the remaining components of CCTV systems so that the security system designer will be able to design an effective CCTV system as part of his overall security system design.

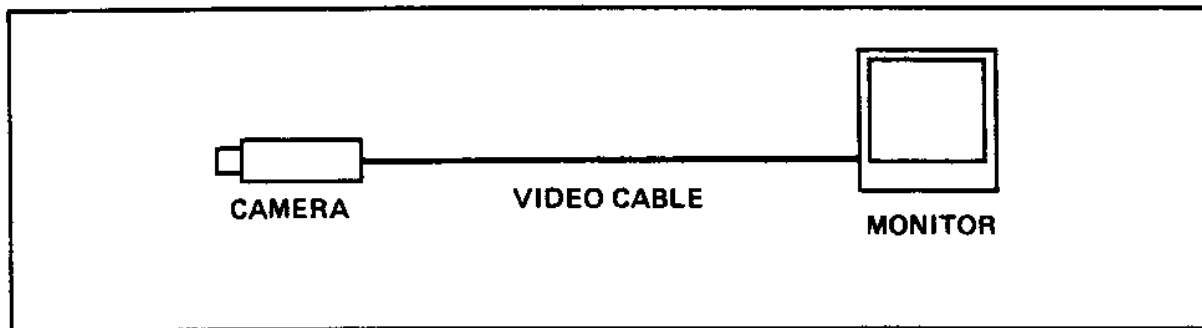


Figure 30
Components of the Basic CCTV System

6.2.1 Cameras. Cameras are the "eyes" of the CCTV system. They are generally classified by "format" and vidicon tube type (or solid state). "Format" is the expression used to denote the size (diameter) of the vidicon tube (or solid state array) in inches. Two formats are generally accepted for security CCTV applications: 2/3 inch and one inch. Two-third inch format cameras are generally used for interior applications, while the one-inch is used for outdoor applications because of the larger image area possible. One-inch cameras generally cost more than 2/3-inch cameras. This is not an absolute rule, since 2/3-inch format cameras are sometimes used cost-effectively outdoors, and one-inch cameras have been used occasionally

for large indoor applications. Cameras used outdoors or in severe environments require protective housings (see paragraph titled "Housings"). Figure 31 depicts these two formats and other camera components. Once format is established, cameras are classified as to vidicon type or solid state. The types of cameras discussed below are currently in use. Camera power requirements are 110 volts ac or 220 volts ac and 24 volts dc. Alternating current is used normally.

6.2.1.1 Standard Vidicon. The standard vidicon tube is the most widely used image tube for CCTV. In 24-hour continuous use, it will last up to 6 months. It is a vacuum tube with a target made of antimony trisulfide

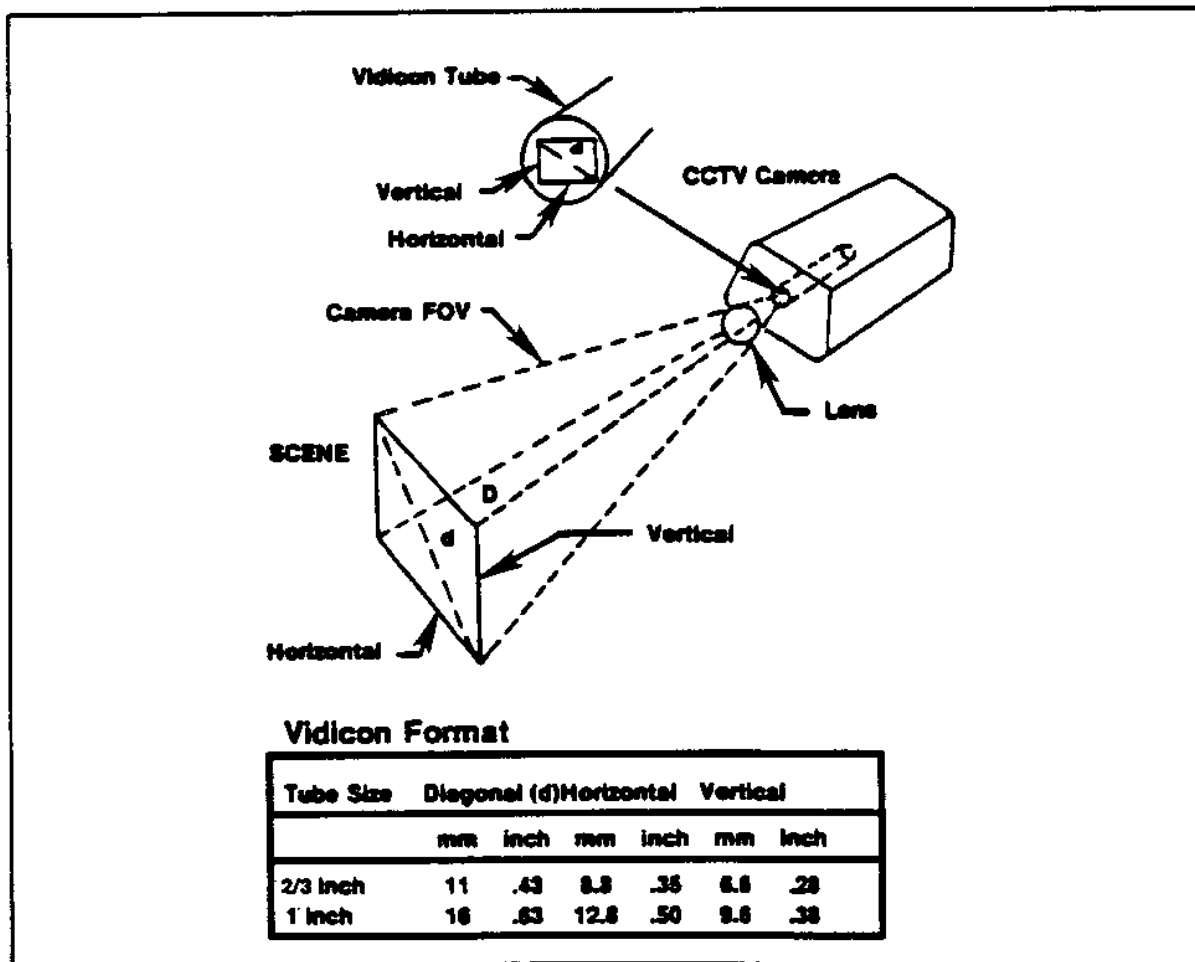


Figure 31
Camera Tube Geometry and Formats

(Sb₂S₃), a photoconductive surface, to form a pattern of different electronic charges which is then scanned by a low-velocity beam of electrons and converted to electronic signals. The standard vidicon light sensitivity range (spectral response) covers the bulk of the visible light spectrum and approximates that of the human eye (see Table 9). Supplemental lighting is required for effective use below one foot-candle (dawn/twilight conditions). A fixed scene may slowly "burn" itself onto a standard vidicon, and direct viewing of a bright light, such as the sun, will cause the target to be burned with subsequent image spotting. The primary disadvantages of standard vidicon cameras are the lighting requirements and their relatively short life, but they are the least expensive and most widely used type of camera.

Table 9
Source Light Level Variations and Applicable Camera Tubes

Illumination Condition*	Illumination (ft cd)	Camera Tube Sensitivity Range†			
		Standard Vidicon	Low Light Level	SIT	ISIT
Direct Sunlight	10,000				
Full Daylight	1,000				
Overcast Day	100				
Very Dark Day	10				
Twilight	1				
Deep Twilight	.1				
Full Moon	.01				
Quarter Moon	.001				
Starlight	.0001				
Overcast Night	.00001				

* Natural light illumination (sun, star, or moonlight) using an f/1.4 lens and viewing a scene with 50% reflectance.

† Shaded region indicates useful operating range of TV camera.

6.2.1.2 Low Light Level. Low light level cameras require less ambient lighting than standard vidicon cameras and generally have a longer life (up to one year). The low light level camera is much more sensitive and produces an effective image for alarm assessment down to light levels which approximate full moonlight (0.01 foot-candles) (see Table 9). Images will not "burn" on these tubes, but their effective use in normal to bright light requires the use of an automatic iris to prevent "blooming" (blinding) of the camera. Low light level cameras use a mosaic target of either a form of silicon, cadmium and zinc teluride or other substance, which gives the increased sensitivity, but otherwise operates like a standard vidicon. Three types are generally available; Newvicon, Ultricon, and silicon diode. Newvicon is a trademark of the Matsushita Electric Company, Inc. Ultricon is a trademark of the Radio Corporation of America. Both are referred to by their registered trademarks rather than their target materials. They are the cameras of choice when available illumination is in the visible spectrum. Ultracon tubes have demonstrated greater reliability in Government agency testing. Silicon diode are the cameras of choice when available illumination is in the infrared spectrum. Infrared illumination often provides better visibility under some fog conditions than would standard illumination. The

low light level type of camera is the general camera of choice for most Navy applications; it has higher reliability and greater operational range than standard vidicon cameras.

6.2.1.3 Very Low Light Level. Specialized applications which have only ambient lighting ranging from starlight upwards (0.0001 foot-candles) are not often encountered. In military applications, they are limited generally to exterior applications where "blackout" conditions are to be maintained at a facility. For such conditions, very low light level cameras which use Silicon Intensifier Target (SIT) or Intensified Silicon Intensifier Target (ISIT) tubes should be considered. These cameras function generally the same as other vidicons discussed above, except that the target materials are extremely light sensitive. Because these cameras are very expensive (over 20 to 30 times the cost of a standard vidicon camera) and have a limited tube life (6 months to one year), it is often more cost-effective to upgrade lighting so that low light level cameras can be used. However, the Navy security system designer may encounter applications where such cameras are appropriate.

6.2.1.4 Solid State Cameras. These cameras are a relatively new development. They use a solid state array such as a Charge Coupled Device (CCD) to serve the purpose of the vidicon tube, and thereby eliminate it. Since the other camera components have used solid state electronics for some time, the vidicon tube has been the CCTV camera reliability "weak point" for several years. Elimination of this vacuum tube increases reliability dramatically as well as minimizing maintenance requirements for the camera's interior components. At present, these cameras cost several times more than a standard vidicon camera and generally provide the same light sensitivity range. Although significantly more sensitive to the infrared and near-infrared spectrum, as this type of camera production increases, its small size and high reliability will make it the industry standard as cost is reduced through increased production. Its use merits serious consideration by the security system designer.

6.2.1.5 Camera Costs. The designated camera should be specified to provide a usable picture under specific operating conditions. Performance is the primary consideration for choosing closed-circuit television components. Secondary to performance characteristics is the consideration of cost. Table 10 outlines some basic data which are important to the design engineering tasks.

6.2.2 Lenses. In order to "see" effectively, a CCTV camera requires an "eye" or lens. How well it can "see" depends upon proper lens selection. How well an object can be seen is determined not only by the illumination or sensitivity of the camera and contrast of the object against the scene background, but also by how large the object is in relation to the entire scene being viewed. Objects less than 1/10 of a degree in angle in a scene cannot generally be identified by an observer. The camera lens determines how large objects appear in a scene. Proper lens selection for each camera is critical in CCTV system layout. Compromises in lens selection may be possible for cost-effectiveness, but if a camera cannot see well, neither will the

alarm station monitor. The discussion in this paragraph will be limited to fixed focal length lenses. Variable focal length or "zoom" lenses will be discussed in paragraph titled "Zoom Lenses."

Table 10
Camera Cost Comparison

Imager Type	Minimum Illumination	Initial [1]	Life [2]	10-Year Cost [3]
VIDICON	1 F/C	\$300	6 mos.	\$2,000
CCD	.3 F/C	\$1200	10 yr.	\$1,200
Low Light	.01 F/C	\$800	1 yr.	\$4,700
SIT	.001 F/C	\$8000	6 mo.-1 yr.	\$26,500
ISIT	.0001 F/C	\$10000	6 mo.-1 yr.	\$37,000

1. Initial cost indicates only the camera and lenses; housings and installation are not included.
2. The life cycle of the camera depends upon lighting conditions in the viewed scene. Reflectance, proper lens operation, pan, tilt and zoom functions, and periodic maintenance also influence the life cycle of the camera.
3. The year cost equals purchase plus anticipated tube replacements.

6.2.2.1 Formats. The area seen through a lens is called the field of view (FOV). Field of view depends upon the distance of the camera from the scene and the scene size. Figure 32 depicts the relative FOV of various lens types. How large an FOV a particular camera at a particular position can have is limited by its format. The format is often the limiting factor in camera lens selection. The FOV of a one-inch camera is about 1/3 larger than that of a 2/3-inch camera with a lens of the same focal length. The focal length is the length of the lens, generally expressed in millimeters. Since the cost of the lens can approach the cost of the camera itself, this illustrates why a one-inch format camera is usually preferred for outdoor applications since a smaller (and less costly) lens can be used. A tradeoff between camera format and cost and lens size and cost is an important part of the design process. Lens speed, or f-stop, is the opening capacity of the lens which determines how much light will be allowed to enter. The f-stop is the focal length of the lens expressed as a function of its diameter ($f\text{-stop} \times d = \text{focal length}$). The more light, the better the camera will see. The smaller the f-stop, the larger the lens diameter is for the same focal length and the more light that passes through the lens. Since most DoD and Navy applications involve cameras with an automatic iris, this factor is less critical than where no automatic iris is used and is not often a consideration for users of this design manual.

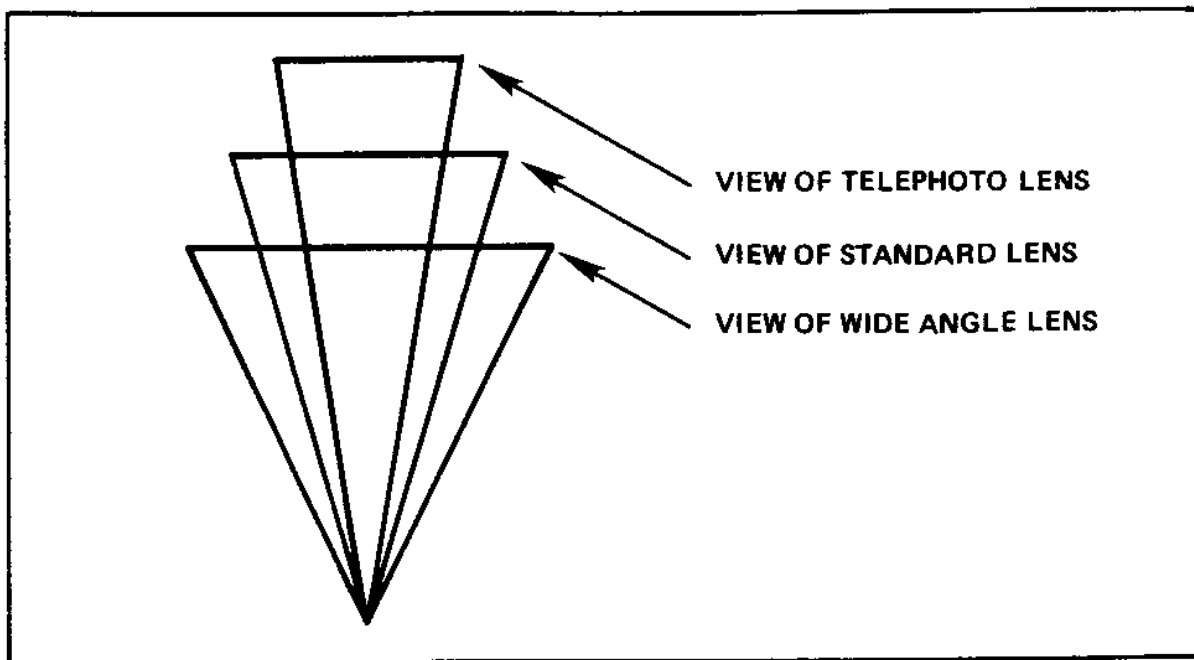


Figure 32
Lens Relative Fields of View

6.2.2.2 Field of View Layout. This is a critical step in CCTV subsystem design. Without a proper FOV layout, the wrong equipment will be specified, perhaps preventing the alarm station monitor from correctly assessing an alarm, causing a costly system failure, and leading to an expensive retrofit. The field of view to be covered by a particular camera should first be measured. Then the correct lens should be selected based upon what format camera is to be used. Table 11 provides a useful guide to lens selection. Many lens manufacturers provide this data on a small pocket slide rule accompanying their advertising literature. If only one-inch format camera data is available, the FOV dimensions required may be multiplied by 1.43 and the result found on the same table to determine the size lens required for a 2/3-inch format camera. If the lens has been selected for a one-inch camera, the focal length multiplied by 0.7 will give the correct size lens for a 2/3-inch format camera. The 25mm lens is considered the industry standard. It is defined as having a magnification (M) of one. To determine the M of a lens, divide the lens focal length by 25 (e.g., a 75mm lens has an M of 3). The FOV of each camera and lens should be carefully laid out on accurate drawings of the facility. These should be confirmed by trial measurements in the field, if possible, ideally using a portable camera set at the selected lens focal length and a video tape recorder (VTR). A single camera/monitor

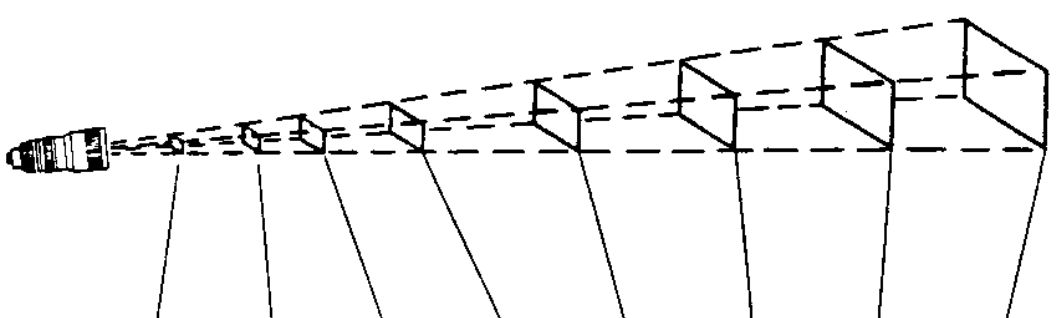
set or a direct view lens may also be used. The scenes can then be analyzed for gaps in coverage, and format and lens tradeoffs can be accomplished. Other considerations are:

- a) Direct view lenses will invert the FOV image. Camera electronics revert it for viewing on a monitor.
- b) One-inch format lenses may be used on 2/3-inch format cameras, but not the reverse.
- c) The focal length of a lens does not change, regardless of the size of the camera vidicon (or solid state array).
- d) A 25mm one-inch format lens has the same FOV as a 16mm 2/3-inch format lens.
- e) The focal length of the lens has an inverse relationship to the FOV. For a wide FOV, a short focal length is required and conversely.
- f) Each camera layout is different, and a standard "system lens" specification may not be possible, but if reasonable tradeoffs can be made, it may be the most cost-effective approach.
- g) As the lens focal length increases, the depth of field, or the distance in the FOV where objects are in focus, decreases. If positive identification of an object is required, this may be an important consideration.

6.2.3 Monitors. Monitors are the devices upon which the CCTV scene is viewed. CCTV monitors generally come in standard sizes of 5, 9, 15, and 19 inches, measured diagonally across the picture. Taking into account the primary requirement of an alarm station monitor to assess a scene only to determine if an intruder is present, Table 12 provides a monitor size selection guide based on documented human factors research. This research says that given a standard TV picture of 525 horizontal lines and 350 vertical lines, a human will generally be able to see an object in a CCTV display if it is from two to seven lines high in the picture. If the requirement increases to positive identification, thus requiring more than seven lines of picture, a larger monitor should be selected. Generally, for access control monitoring, pan/tilt/zoom (PTZ) surveillance, and other "close in" work, the 19-inch monitor is preferred. The 9-inch monitor is used for most DoD security applications for alarm assessment. The configuration of monitors is generally in stacked sets of two maximum per alarm zone (other services use up to five in a horizontal row) and is a matter of debate among human factor engineers. It is generally accepted, however, that one operator can effectively handle data from no more than eight monitors (four sets of two stacked vertically)

for alarm assessment and that PTZ controls add additional burden to the operator, which may be detrimental in times of stress such as multiple alarm situations. If more than four alarm zones can alarm simultaneously, VTR should be used for later assessment. It is also accepted practice for DoD application that monitors for alarm assessment shall be blank until an alarm occurs or, if being used for operator surveillance of an area, that the alarmed zone scene automatically replace what is on the monitor. Care in monitor size selection and careful alarm monitor station integration must be the prime considerations of the security system designer so that the CCTV monitors do not overburden the operator's senses with the amount of the other data also being presented.

Table 11
Lens Application Guide

APPROXIMATE FIELD OF VIEW FOR SEVERAL COMMONLY USED LENSES AT VARIOUS DISTANCES FROM LENS TO SUBJECT									
RULES FOR USING LENSES 1. 1" Format Lenses work on 1" or 2/3" Format Cameras. 2. 2/3" Format Lenses should only be used on 2/3" Format Cameras. 3. The focal length of a lens does not change regardless of the size of the camera pick-up tube. 4. A 25mm lens on a 1" Format Camera has the same field of view as a 16mm lens on a 2/3" Format Camera.									
									
1" Format Camera	Horizontal Angle of View	5' W x H	10' W x H	15' W x H	20' W x H	30' W x H	40' W x H	50' W x H	100' W x H
6.5mm	103°	9.8' x 7.2'	19.2' x 14.4'	28.8' x 21.6'	38.4' x 28.8'	57.6' x 43.2'	76.8' x 57.6'	96' x 72'	192' x 144'
12.5mm	54°	5' x 3.75'	10' x 7.5'	15' x 11.25'	20' x 15'	30' x 22.5'	40' x 30'	50' x 37.5'	100' x 75'
25mm	28°	2.5' x 1.87'	5' x 3.75'	7.5' x 5.62'	10' x 7.5'	15' x 11.25'	20' x 15'	25' x 18.75'	50' x 37.5'
50mm	14°	1.25' x 0.94'	2.5' x 1.87'	3.75' x 2.81'	5' x 3.75'	7.5' x 5.62'	10' x 7.5'	12.5' x 9.37'	25' x 18.7'
75mm	9°	0.83' x 0.63'	1.67' x 1.25'	2.5' x 1.87'	3.33' x 2.5'	5' x 3.75'	6.67' x 5'	8.33' x 6.25'	16.7' x 12.5'
100mm	7°	0.62' x 0.46'	1.25' x 0.94'	1.87' x 1.4'	2.5' x 1.88'	3.75' x 2.81'	5' x 3.75'	6.25' x 4.69'	12.5' x 9.4'
150mm	4° 36'	0.42' x 0.32'	0.83' x 0.63'	1.25' x 0.94'	1.67' x 1.26'	2.5' x 1.88'	3.33' x 2.5'	4.17' x 3.13'	8.3' x 6.3'
300mm	2° 18'	0.21' x 0.16'	0.42' x 0.32'	0.62' x 0.46'	0.83' x 0.62'	1.25' x 0.94'	1.66' x 1.21'	2.08' x 1.56'	4.2' x 3.2'
2/3" Format Camera	Horizontal Angle of View	5' W x H	10' W x H	15' W x H	20' W x H	30' W x H	40' W x H	50' W x H	100' W x H
4.5mm	100°	11' x 8.2'	22' x 16.4'	16.5' x 12.3'	22' x 16.4'	33' x 24.6'	44' x 32.8'	55' x 41'	110' x 82'
9.0mm	52°	5.5' x 4.1'	10' x 7.5'	15' x 11.2'	20' x 15'	30' x 22.5'	40' x 30'	50' x 37.5'	100' x 75'
12.5mm	38° 47'	3.5' x 2.6'	7' x 5.25'	10.5' x 7.9'	14' x 10.5'	21' x 15.75'	28' x 21'	35' x 26.2'	70' x 52'
17mm	29°	2.9' x 2.2'	5.8' x 4.4'	8.7' x 6.6'	11.6' x 8.8'	17.4' x 13.2'	23.2' x 17.6'	29' x 22'	58' x 44'
25mm	18° 30'	2.0' x 1.5'	3.5' x 2.5'	5.2' x 3.9'	7' x 5'	10.5' x 7.5'	14' x 10'	17.5' x 13.3'	35' x 26'
35mm	14° 30'	1.4' x 1'	2.8' x 2'	4.2' x 3'	5.6' x 4'	8.4' x 6'	11.2' x 8'	14' x 10'	28' x 20'
50mm	9° 15'	.84' x .63'	1.67' x 1.25'	2.5' x 1.87'	3.25' x 2.44'	5' x 3.75'	6.5' x 4.9'	8.3' x 6.25'	17' x 12.5'
75mm	6° 10'	.58' x .43'	1.1' x .975'	1.63' x 1.22'	2.16' x 1.62'	3.25' x 2.44'	4.3' x 3.2'	5.5' x 4.13'	11' x 8.25'

6.2.4 Options for Enhanced Capabilities.

6.2.4.1 Zoom Lenses. For surveillance applications where the FOV should be varied, use of a motorized automated adjustable FOV or "zoom" lens is appropriate. The variable focal length of the zoom lens permits change in FOV without change in lenses. Many models are available, but generally a five to 10 times change is possible for the FOV and is accomplished by operator remote control. At the same time, as the lens "zooms" in or out, the depth of

Table 12
Monitor Size Selection

VIEWING DISTANCE	RECOMMENDED MONITOR SIZE
LESS THAN 14"	5"
14" - 36"	9"
36" - 60"	15"
50" - 76"	19"

field (objects in focus) will also change and will also require operator adjustment. For that reason, zoom lenses are generally not suitable for near real time alarm assessment purposes. Automated devices, called "shot boxes," are available which will automatically return a zoom lens to a particular setting when not under operator control or upon alarm in the zone covered by the camera. This should be the only acceptable method for the system designer to apply a zoom lens camera as an alarm assessment camera. Since zoom lenses cost two to 10 times more than fixed focal length lenses and the shot box is also an added cost, careful cost-effectiveness analyses should be completed prior to selection of a zoom lens option for alarm assessment.

6.2.4.2 Tilt and Pan. Tilt is the movement of a platform up and down. Pan is side-to-side movement (see Figure 33). Tilt and pan CCTV camera mount

platforms are appropriate selections for increasing the effectiveness of CCTV surveillance cameras. Because of the relatively slow movement accomplished, even with a shot box, they are usually considered unacceptable for near real time alarm assessment applications. For surveillance applications, platforms, in combination with a zoom lens, can be a most cost-effective application by increasing the FOVs of individual CCTV cameras. Models of tilt and pan platforms are available for every conceivable application from interior to outdoor on carrier flight decks. The system designer should keep in mind, however, that these are mechanical devices and require continual maintenance to assure proper operation. Models with sealed lubrication are best for all applications to minimize maintenance man-hour costs, although they are more expensive. Careful cost-effectiveness analysis is required before selection of tilt and pan (and zoom) options over additional fixed cameras to provide the coverage(s) required.

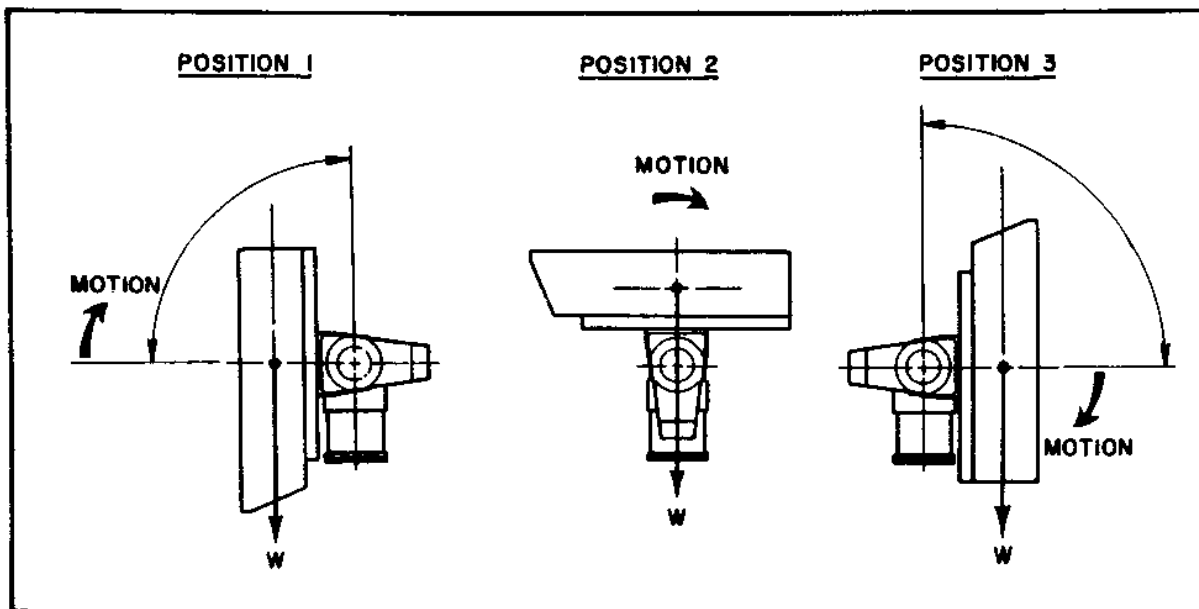


Figure 33
Tilt and Pan Motions

6.2.4.3 Housings. CCTV cameras are generally manufactured for indoor use in benign environments. For use in indoor applications where vandalism may be a problem or other tampering is likely, and for outdoor applications, a camera housing is required to protect the camera so it will function properly under such unbenign conditions. Specialized cameras are manufactured for specifically harsh applications such as for monitoring the interior of nuclear reactors, but the only effective solution for such environments is very expensive. The "requirement" for camera housing comes from the fact that using such an item with a camera manufactured for a less harsh environment has proven to be the most cost-effective approach. The Navy security system designer is faced with a wide spectrum of applications

for CCTV, but in

13.02-93

general, the vast majority will involve the use of camera housings. The designer should also keep in mind that major U.S. CCTV system manufacturers do not make their own camera housings, so that while housings may be listed in their catalogs, it is often more cost-effective to procure the housing(s) from the housing manufacturer. Housings come in all shapes and sizes for all applications and in varying price ranges. Figure 34 depicts some of the more commonly used housings found in DoD and Navy applications. Key considerations for the designer are:

a) The primary purpose of housings for interior applications is to provide tamper protection and limited environmental protection. If the threat is so great that the housing requires a tamper alarm (usually a BMS), then it should be connected to the IDS system as a separate type of zone indication. Since some housing devices for environmental control are mechanical in nature (windshield wipers, blowers, etc.), the indoor ambient environment should be examined very closely so that only those required are specified. Over-specification of such devices is a common error which has adverse consequences in maintenance and spare parts expenses.

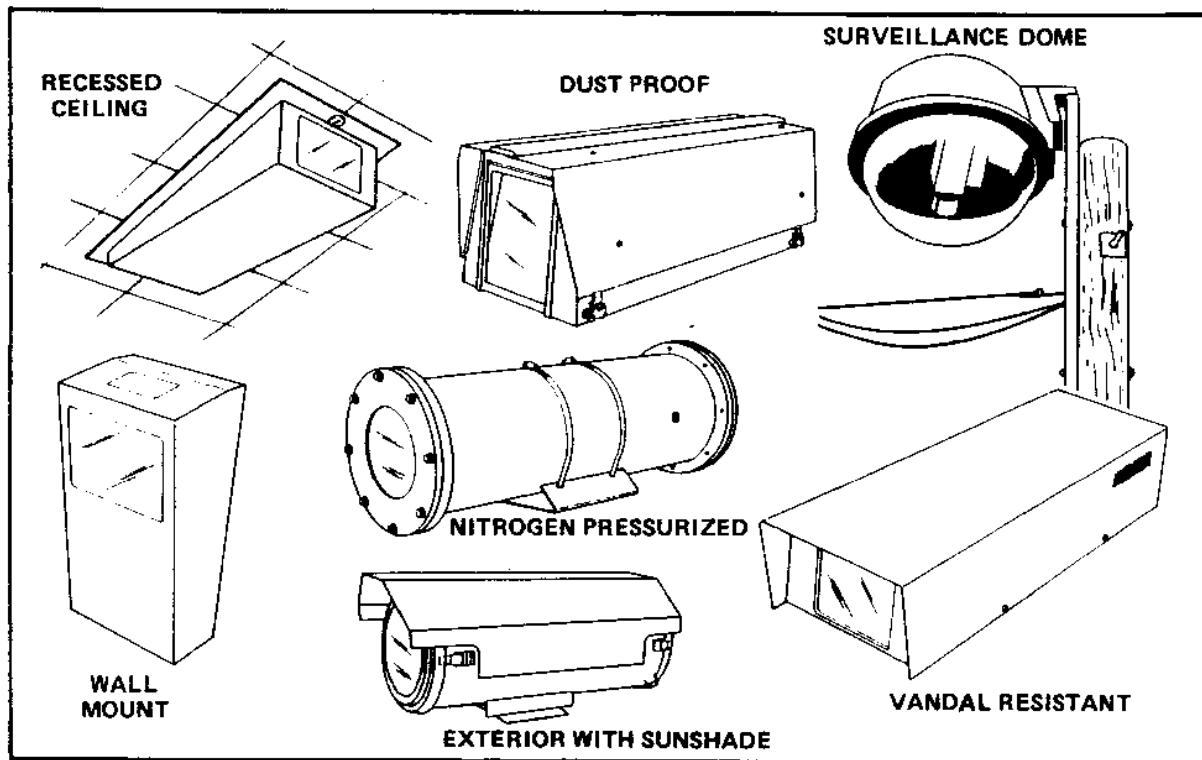


Figure 34
Camera Housings and Enclosures

b) Outdoor applications may require the full range of environmental housing protection devices. However, the system designer should consider carefully the lower hardware costs with high maintenance levels required of standard commercial housings which use mechanical fans for heating/cooling, windshield wipers, etc. versus the higher hardware costs with lower maintenance levels required for nitrogen pressurized housings which do not require mechanical devices for environmental protection. Life cycle cost analysis should be a serious consideration factor.

c) The ambient environment may dictate the type of housing required. Strong sunloading in exterior applications may require the use of a sunshade. High atmospheric dust content dictate no mechanical elements due to lens scratching from windshield wipers, etc. The designer must consider all aspects of the application in selecting a camera housing.

d) Dome housings are often used for surveillance applications. In addition to being tamper resistant and providing environmental protection for both the camera and PTZ mount, domes are generally equipped with smoked or one-way glazing. This has the advantage of persons in the FOV not being able to discern that the camera is "looking" in their direction. Domes generally cost more than other enclosures, but are sometimes considered worth the extra cost for specific applications.

6.2.4.4 Mounting. Two types of mountings are of concern for the CCTV subsystem designer: lens mount and assembled camera mount (and housing). For lens mounting, the "C" mounting is the industry standard. It is a screw-in mount and has a sleeve one inch in diameter with threading of 32 threads per inch. Most lenses, even for specialized applications such as concealed pin holes, are manufactured to this standard. Camera mounts are available in many sizes and shapes and, like housings, are not manufactured by the U.S. CCTV system manufacturers. Procurement of housing and mount from the same manufacturer will assure proper mounting hardware alignment. The prime consideration in camera mount selection is that the mount must sturdily support the camera/lens/housing configuration. Vibrations, pole movement, etc. will be magnified on the displayed CCTV picture. Wind loading on larger camera housings should also be considered. Some large lenses put an undue strain on lighter mountings, particularly with PTZ platforms affixed. In camera mountings, the designer should remember that for most Navy applications, heavy-duty camera mountings are most cost-effective. Skimping in this area is false economy. For fenced perimeters, if existing buildings, poles, etc. are unsuitable, specialized camera poles with mounting included are available. The descriptions and specifications of these items are available from the Naval Electronics System Engineering Activity, St. Inigoes, MD 20684. This agency should also be contacted for assistance on any large scale exterior CCTV system design and procurement. The following additional design considerations apply:

a) When computing the camera mount required, the total weight of all components should be used. To this, an additional one to 2 pounds should

be added for cable. For outdoor applications, one to 7 pounds each should be added for wind and snow loading. The mount has to carry the total weight.

b) Wall and ceiling mounts are recommended for indoor use; wall and pedestal mounts for outdoor use. In PTZ applications, the clearance required by the entire mounted unit is a large mount size determinant.

c) Many manufacturers make similar quality mounts; not all mounts fit all camera brands; prices vary between manufacturers; comparison shopping is advised before final specification.

6.2.4.5 Video Recorders. Also known as video tape recorders or "VTRs," these devices are used for event recording as discussed in paragraph titled "Event Recording." (Video disc and solid state video recordings are relatively new technologies which are not presently in general use for CCTV security applications and consequently will not be discussed in this design manual.) Real time recording of alarm zone scenes is generally reserved for alarm situations. Most VTRs operate in a time lapse mode for access portal and other activity monitoring and in a real time mode for sensor alarm queued situations. In this manner, over 100 hours of elapsed time can be selectively compressed onto one 2-hour tape. Three different kinds of VTRs are generally available: 1/2-inch reel-to-reel; 1/2-inch cassette; and 3/4-inch cassette. Generally, the reel-to-reel models have been available longer than cassette models and are specifically available for security applications. The prime disadvantage of reel-to-reel models is that tape handling is required for threading prior to recording. Attendant damage and missed recordings have resulted in the cassette models being the general models of choice for DoD and Navy applications. The 3/4-inch tape generally provides a higher quality picture with present technology. The system designer should consider that, like an operator, a VTR can also go into an overload condition when too many cameras are in an "alarm" state. Generally, for large systems (over 40 cameras) where alarm activity is high, a second VTR is recommended. A recommended option for a VTR is a time/date generator which superimposes that data on the tape picture. This is required for introduction of the recording as court evidence and is useful for command review of events. Sensor zone labelling is also possible if desired, but is not required for evidence purposes. Such generators are often used for alarm station monitor orientation. A less expensive alternative is to have an unobtrusive sign in each camera FOV with the sensor zone designation. The system designer should consider the VTR as an option when pictorial event recording is a necessity. For most applications, the record provided by the hard copy record of a printer will suffice for security management purposes. For larger systems, a VTR is often a cost-effective supplement for management purposes.

6.2.4.6 Switching Equipment and System Integration. Video switchers enable the cost-effective use of multiple cameras with a few monitors. The ergonomic (human factors) benefits are also well documented. Generally, for any CCTV system with over a few cameras, the cost of a video switcher is a clear advantage over the costs associated with dedicated monitors and an operator overload. When two or more cameras are used in a system, a switching device may be employed. For two camera systems, for example, a manual or passive

system may be employed which, by operator manual control, switches the output of two to four cameras between one monitor. For systems of four cameras or more, an automated switcher is generally employed. The various features which a sequential switcher may incorporate are defined in Table 13.

6.2.4.7 Switchers Features. The homing option automatically advances the picture on a single monitor at a predetermined interval, selectable from one to 45 seconds. Bridging permits two outputs, one for sequential viewing of all cameras as in a homing switcher and the second for continuous viewing of a selected camera. Looping allows the inputs on a switcher to be fed to another device such as a VTR, monitor, switcher, etc. Automatic or alarm-programmed assures that the scene of a sensor zone in alarm will be displayed as an override to any other display. Figures 35 through 38 display the control switch positions for operating homing, bridging, and looping switcher options as stand-alone options for a simple CCTV system, as well as the common looping/bridging combination (Figure 38). The alarm option would naturally assure automated alarm zone viewing of the camera scene(s) by the appropriate monitor(s). The combination illustrated in Figure 38 could also have provided for output to a VTR rather than a second monitor location. Table 14 provides a guide for switcher option selection and system integration general guidelines. For most Navy applications, use of a video switcher is the most cost-effective and ergonomic-dictated approach. Use of one which incorporates bridging and auto-alarm options is probably the most common approach to both assure automatic alarm assessment and permit operator scene selection for surveillance or assessment of adjacent zones to the alarmed zone. Use of a VTR will require incorporation of the looping option. Using Table 14 as a

Table 13
Sequential Switcher Definitions

DEFINITIONS

THE FEATURES AVAILABLE FOR A SEQUENTIAL SWITCHER ARE DEFINED BELOW:

HOMING: A TYPE OF SEQUENTIAL SWITCHER WHICH ALLOWS CONTINUOUS VIEWING OF ANY NORMALLY SEQUENCED CAMERA INPUT ON A SINGLE MONITOR.

BRIDGING: A FEATURE WHICH PERMITS A SEQUENTIAL SWITCHER TO CONTINUOUSLY DISPLAY ONE CAMERA INPUT ON A SECOND MONITOR.

LOOPING: A VIDEO OUTPUT CONNECTOR IS PROVIDED FOR EVERY CAMERA INPUT TO ALLOW THE VIDEO FROM ANY CAMERA TO BE FED TO ANOTHER SWITCHER OR ANOTHER DEVICE.

ALARM PROGRAMMED: THE AUTOMATIC SWITCHING OF A SEQUENCED CAMERA INPUT ONTO A MONITOR UPON CLOSURE OF AN EXTERNAL ALARM SWITCH.

guide, the system designer should be able to configure the proper system control components for alarm assessment. Switchers are available from several manufacturers with the capabilities required. Maximum camera capacity varies from eight to 64 cameras. The various models available provide for modular expansion to meet future needs. Once again, life cycle cost analysis will determine which approach to take - purchase of a "large" capacity system or multiple units, each with a smaller capacity. This factor must be considered with the other considerations discussed in this section. Figure 7, Section 2, depicts the various elements which the designer can consider, some of which are discussed below and in Section 7. Only after consideration of the full range of options, however, can the security system designer properly design the IDS assessment subsystem.

6.2.5 The Role of Lighting in CCTV Effectiveness. The design of lighting systems is not within the scope of this design manual. The brief discussion herein is only intended to identify for the CCTV subsystem designer the lighting factors which should be considered in the assessment subsystem design. An excellent detailed treatment of security lighting design guidance is contained in the Lighting Study for CCTV at Naval Security Group Sites, published by the Atlantic Division, Naval Facilities Engineering Command in June 1983. Key application considerations for the designer are:

- a) Lighting improvements have proven more cost-effective generally in security system design than expensive investments in very low light level cameras.

- b) The type of lighting selected depends upon several factors. The optimum light range of various camera types is often a significant factor. Figure 39 provides a graphic representation of the relationships involved between camera vidicons and various artificial and natural lighting sources.

- c) Lighting has a deterrent effect. The purpose of most lighting upgrades is (or should be) to eliminate places of concealment.

- d) For CCTV applications, good contrast is most important for intruder presence determination under marginal lighting conditions. New techniques such as the use of retroreflective materials in clear zones should be considered, as should the fact that low pressure sodium lighting provides poor contrast.

- e) The designer should keep in mind that fluorescent lighting, the most common DoD and Navy interior lighting source, is a source of nuisance alarms to some sensors (see Section 4, paragraph entitled "Volumetric Sensors-Interior"). A trade-off may have to be made between IDS element selection and performance and lighting type selection.

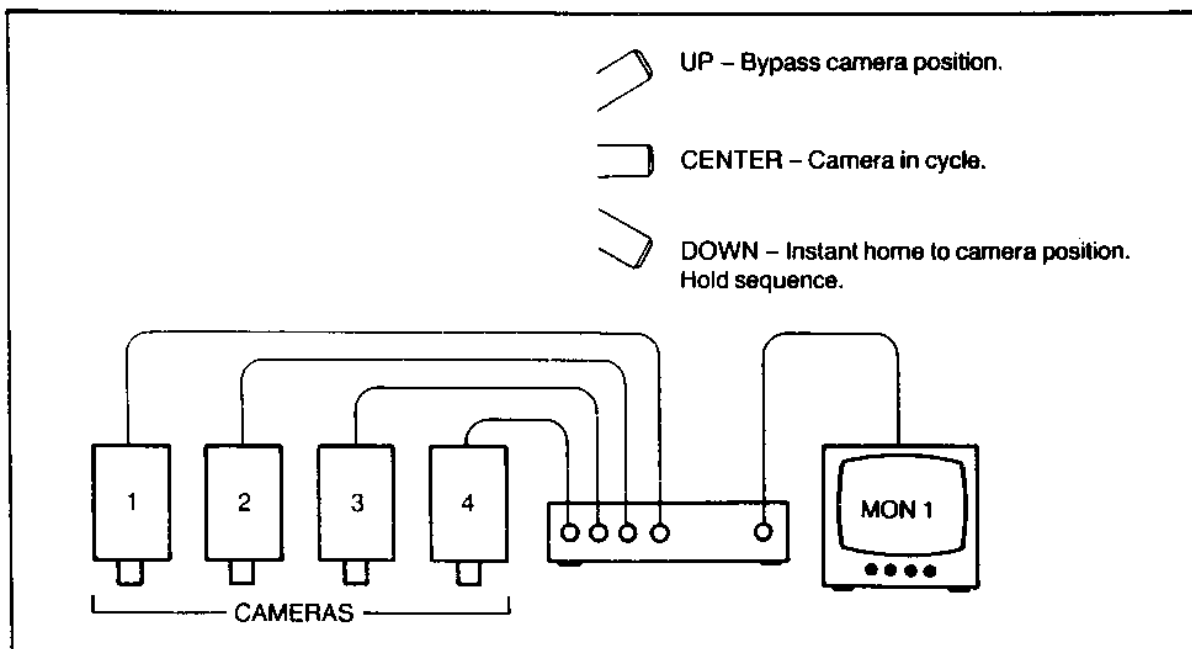


Figure 35
Homing Sequential Switchers

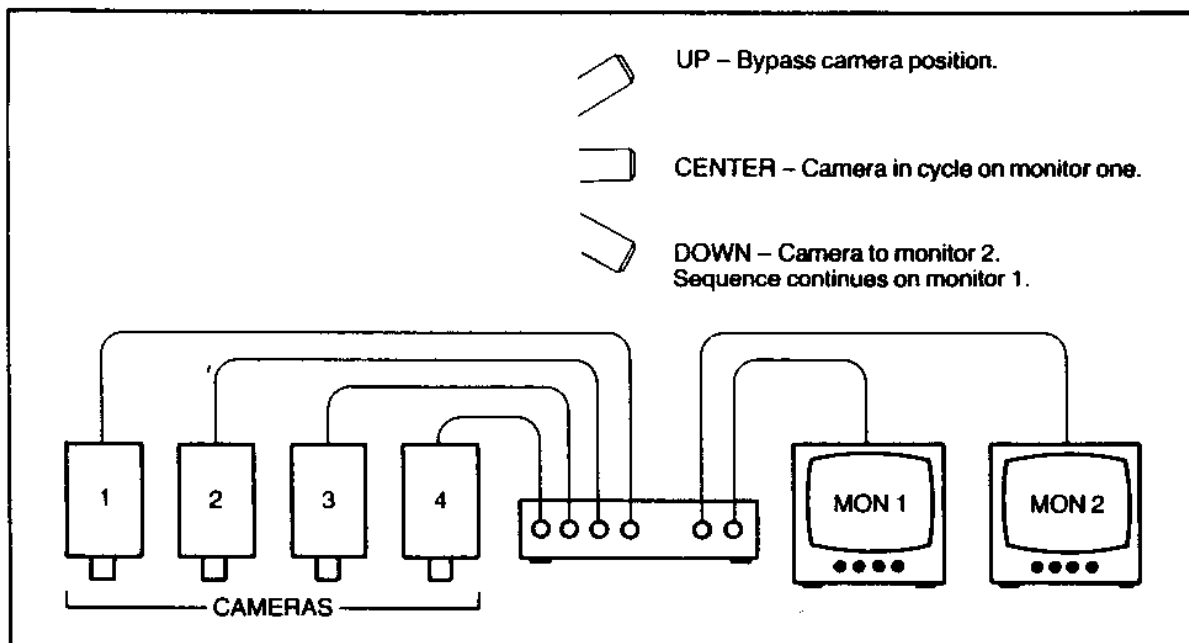


Figure 36
Bridging Sequential Switchers

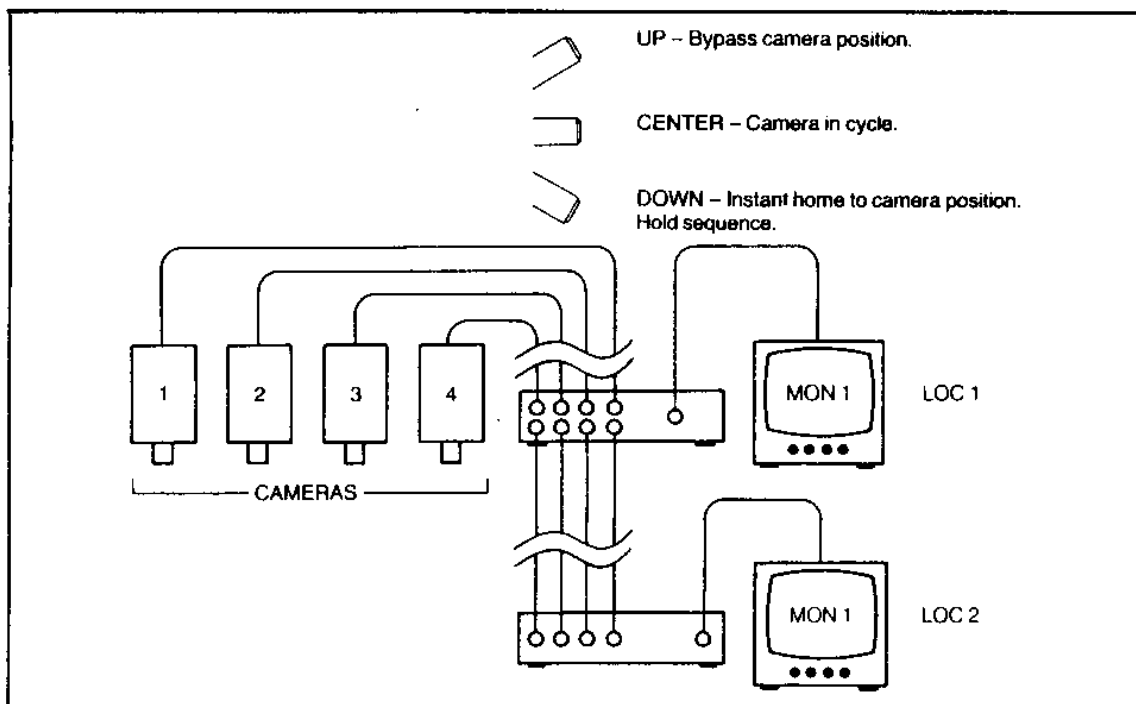


Figure 37
Looping Sequential Switchers

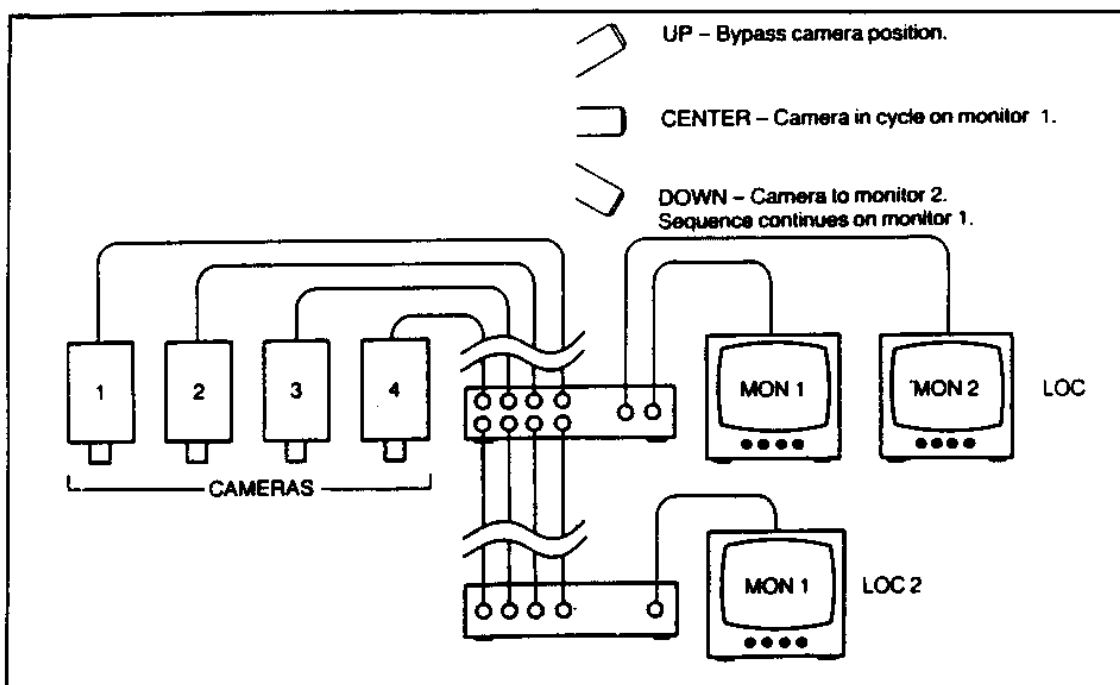


Figure 38
Looping/Bridging Sequential Switchers

Table 14
Switcher Selection Guide

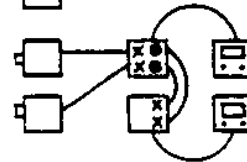
Passive Manual Switcher —

This type switcher remains fixed to one video input until operator depresses a button to select a different input for viewing.



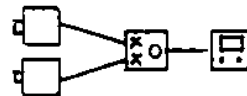
Manual (passive) Two Position Switcher

Manual Looping Input Switcher. (Both monitor locations have separate and independent control over input to be used.)



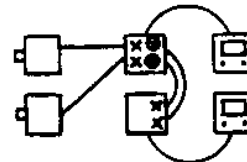
Homing Sequential Switcher —

Automatically advanced from one to another camera per predetermined dwell time sequence. Adjustable dwell time is generally 1-45 seconds.



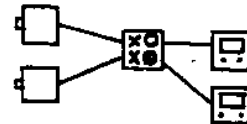
Looping Input Homing Sequential Switcher—

Looping outputs allow for additional monitoring stations with independent control for both operators.



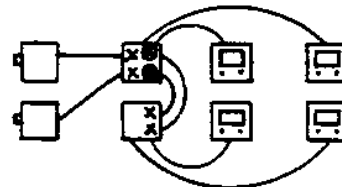
Bridging Output Sequential Switcher —

Two outputs. First monitor always maintains sequence of all cameras, and second monitor output is the hold (or continuous view) for selected camera input.



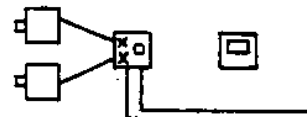
Looping Input Bridging Sequential Switcher —

Looped inputs on this bridging output sequential switcher allow additional monitor stations. Switcher operation at both locations totally independent.



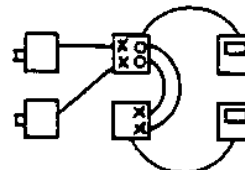
Auto Alarming Sequential Switcher —

Allows switcher to be adapted to a burglar alarm system. When activated will cause area covered by respective camera to be automatically switched onto monitor and an alarm buzzer sounded. Feature available on most homing and bridging type switchers.



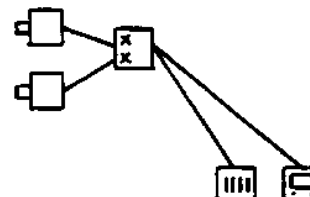
Auto Alarming Sequential Switcher

Both types of alarm switchers are available in looped input variations. Area entered will take priority over previous selected functions, such as hold selection.



Remote Switcher —

Should cameras be a great distance from monitor, it may be cost effective to remote switch functions (and bring back only one or two video signals). Command functions are carried over intercom type wire with full operator control of the switcher. Homing and bridging type switchers are available in remote configuration (both terminating and looping inputs).



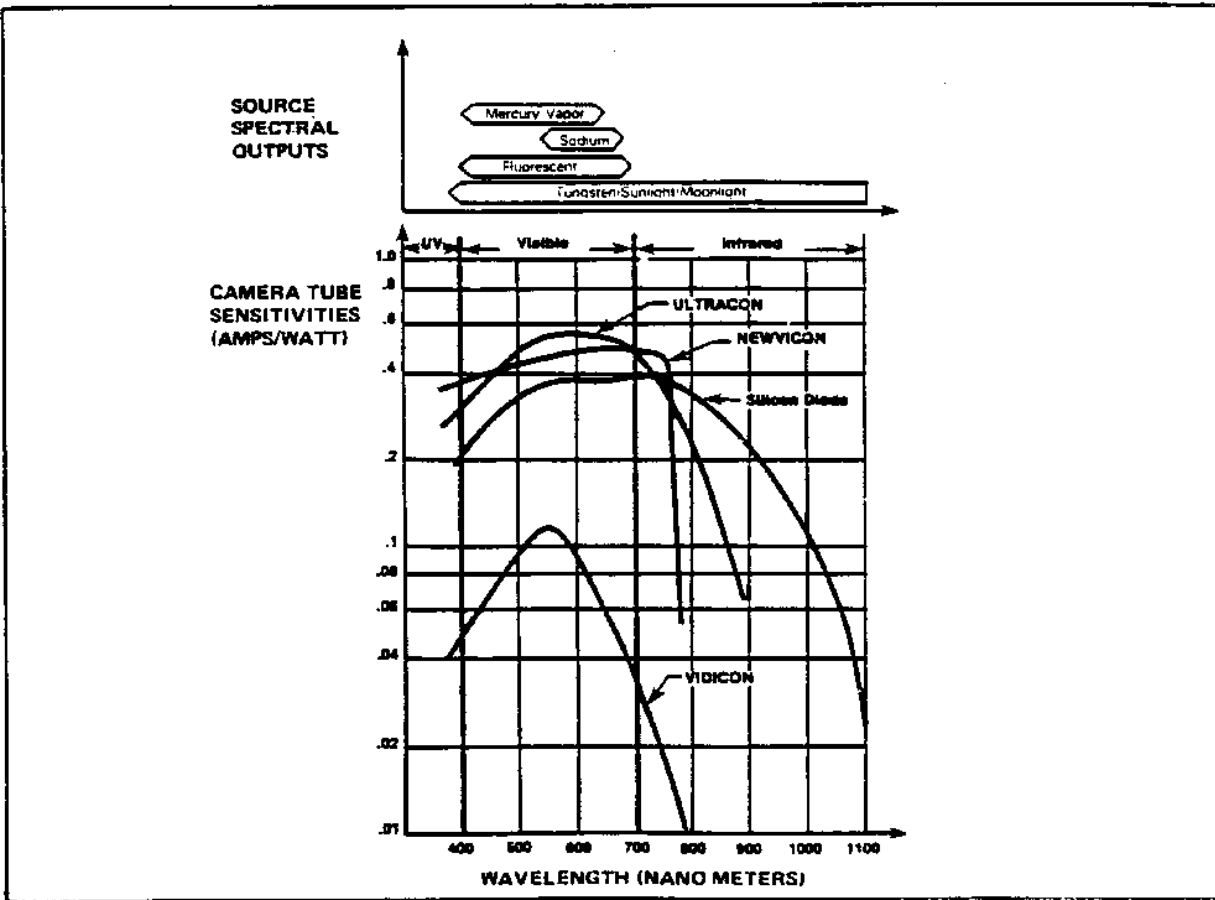


Figure 39
Natural and Artificial Light Source Versus Camera Tube Sensitivities

Sensitivities]

13.02-102

Section 7: ALARM SIGNAL

COMMUNICATIONS

7.1 Criticality of Communications in System Integrity. Electronic intrusion detection is accomplished by employing sensors of various types as discussed in Section 4 of this design manual and communicating the information to the security organization for definitive response. IDS communications serve to take sensor detection data and present it in human-readable form to permit assessment and resolution of factors that caused the detection. The penetration or disruption of communication during this phase of the alarm sequence is critical because the occurrence will not appear to the monitoring personnel as an alarm. Integrity of the system is obviated in the event of data communications failure.

7.2 Types of Communications Links. Communications of intrusion detection systems involves the third step of the sense, control, and signal process. This process requires further input by personnel for the mission of security. The knowledge of intrusions and intrusion attempts must be communicated from the sensor to the monitoring/display in a clear, speedy manner which is resistant to compromise and conducive to rapid fault detection and repair. Wire, microwave, radio frequency and, most recently, fiber optics may carry the electronic, voice, or video communications with the protection required for security operations.

7.2.1 Hardwire/Landline. Hardwire or landline communications is typically a physical wire connection from point-to-point. The size, type, and number of conductors vary according to the sense devices, control instrument, and reporting display. The type of signal transmitted and the susceptibility of that signal to compromise will dictate the need for protection from the environmental and man-initiated degradations of the information signal.

7.2.1.1 Sensor Data. Communication from the detection sensor is most commonly carried on wire. The two principal types of this data are: the interruption of a stream of current through a loop normally closed (N.C.) circuit and the passage of a stream of current (or detection of continuity) in a loop-normally open (N.O.) current. The normally closed (N.C.) circuit is depicted in Figure 40; the normally open (N.O.) circuit is depicted in Figure 41. The indication of detection results from a change of state in the line. There are limitations to the circuit designs, particularly if more than one contact device is on a single line. The approach of more than one device on the line is termed "daisy chain." The Figure 42 local hardwire depiction is indicative of the unique problem of identification of device(s) in alarm. Any one of the detectors in alarm is indicative of a single general alarm condition, requiring additional investigation to determine the device in alarm. The daisy-chain loop approach does not direct immediate attention to the point of intrusion and is not recommended for IDS implementation at Department of Navy facilities. The recommended wiring technique is point-to-point, single line from detection device to control unit. Wire is the most commonly used media for the transfer of point-to-point information

communications. Often, the success of the security process relies exclusively on this communication system for intrusion and attempted intrusion notifications. The two principal wiring types used with the IDS are proprietary and telephone lines. Both of these permit low-voltage circuits in multiples of pairs of wires.

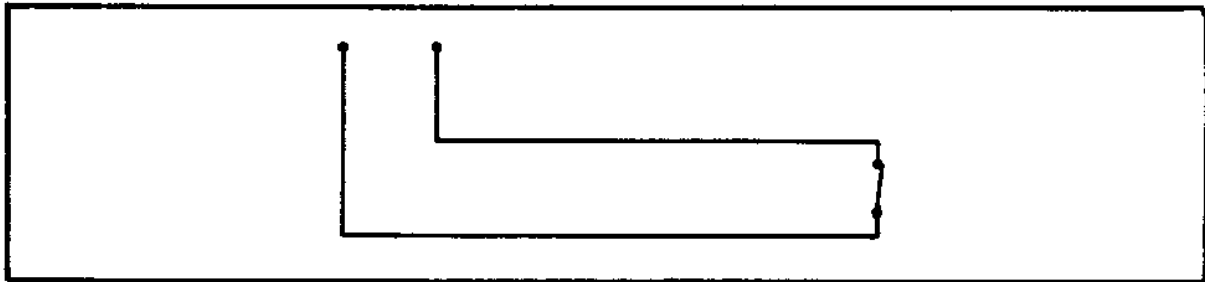


Figure 40
Normally Closed (N.C.) Circuit

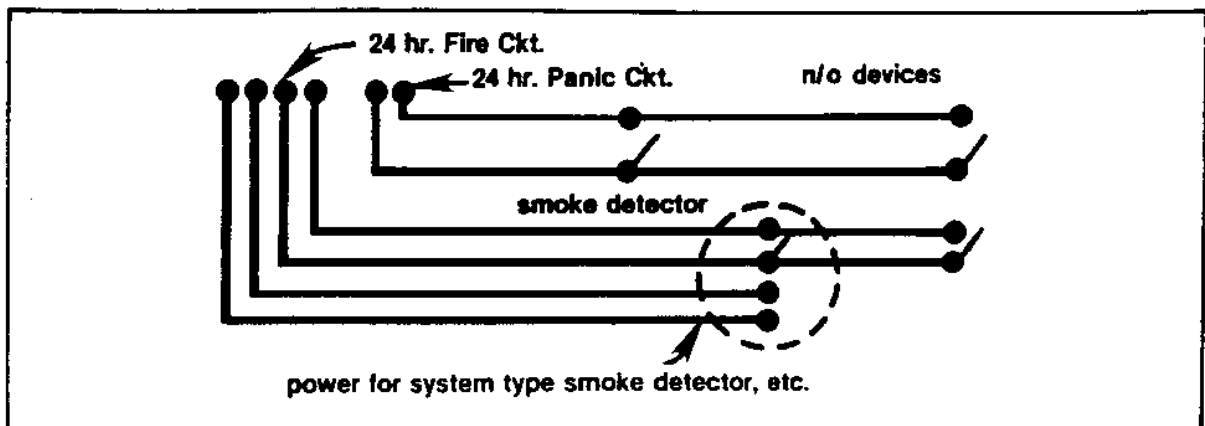


Figure 41
Normally Open (N.O.) Circuit

7.2.1.2 Video Data. The communication link between camera and monitor in the simple closed-circuit television system is most often on hardwire, coaxial cable networks. This cable provides shielding and grounding characteristics that are critical for video signal quality. Degraded signal conditions can

often be improved by using video amplifiers. It is generally more economical to use standard coaxial cable and an amplifier for greater distance transmission than substituting types of cable. Figure 43 and Table 15 depict typical closed-circuit television wiring schemes and distance constraints.

7.2.1.3 Controller Data. After the normally open and normally closed circuit information is processed by a controller, this information is transmitted by various techniques to either a terminal (printer or video display) or a computer. The information or data transmission is in the form of audio pulse, tone, or electrical current. Various equipment uses specific wire types, shielding, or numbers of conductors, or provides easy methods to prepare the information for fiber optic, multiplex, microwave, or telephone line modulation/demodulation techniques. Most data communication techniques require specifically conditioned wire circuits to carry the signals.

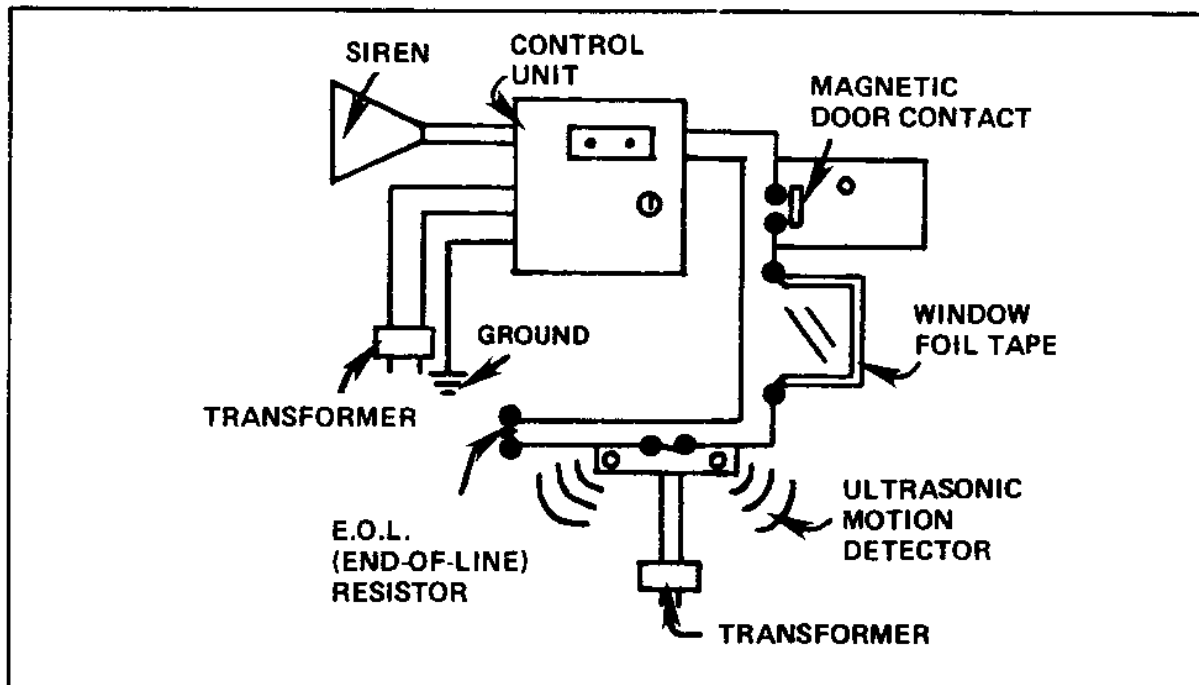


Figure 42
Typical Local Hardware IDS Communications Configuration

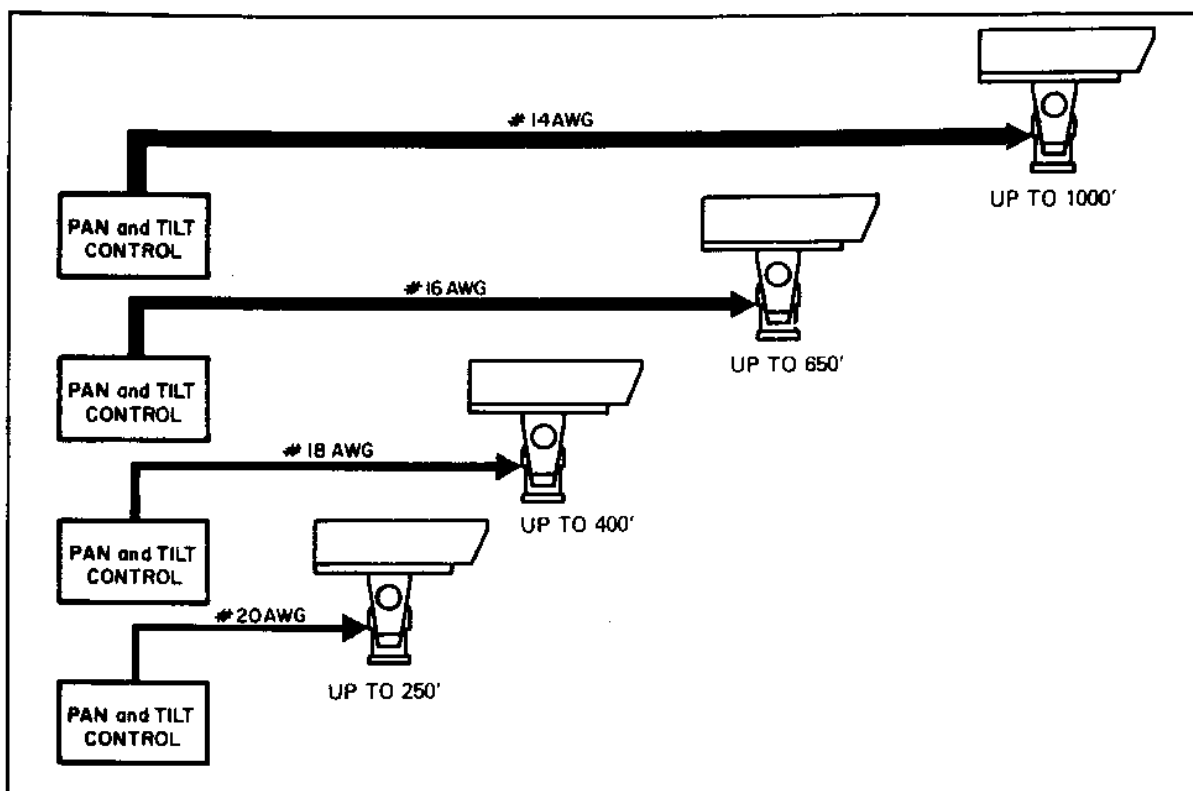


Figure 43
Direct Wire Hookup (CCTV)

Table 15
CCTV Coaxial Cable Characteristics

Cable Type	Maximum Recommended Camera to Monitor Range for Each Type Cable[*]		
	Cable Only ^{L1}	With Video Amp. ^{L2}	Powered ^{L3} Coax
Rg 59/U	500 ft.	3400 ft.	2000 ft.
Rg 6/U	750	4800	
Rg 11/U	1000	6500	3000 ft.
Rg 15/U	1500	8600	

NOTES:

[1.] All Cables have a 75 [phi]hm impedance necessary for CCTV.

[2.] The video amplifier is connected at camera output to extended the coaxial cable

twisted pair of telephone wires. A special transmitter and receiver perm transmission over a range of 4000 ft. using No. 22 or No. 24 wire.

[3.] Single coaxial cable powers th

effective range.

camera and transmits the video signal

[*] If a coaxial cable can't be installed, the video signal can be transmitted over a

7.2.2 Proprietary Installations. The wholly owned and maintained wire networks within a facility or group of facilities are considered to be proprietary. These networks, when properly maintained, represent the greatest amount of system control and responsibility to the user. The electronic on/off or voltage pulse communications are sent by the detector to the control unit. Control unit communications are sent to the reporting and display components of the IDS (see Section 8). All of these communications will require some proprietary wire networks.

7.2.2.1 Loops. Loop communication networks consist of a pair of wires laced through an area or building with devices connected at intervals. These devices or subsystems report on this signal line pair to the controller and, subsequently, the display. A simple example of this scheme is depicted in Figure 42. There is a coding technique to differentiate devices on the single line pair. The party-line or McCulloch coding methods permit each device to send a specific signal, at any time, along the wire pair loop to the controller. These discrete signals are interpreted by a receiver and subsequently displayed. The disadvantages in using this type of coding technique are that any fault in the line cuts off all "downstream" reporting devices, and that two simultaneous reports on the line will be indecipherable. The single most significant fault is the "clash" or simultaneous report which can serve to frustrate monitoring personnel who know that there are alarm conditions but do not know which devices are reporting. Loop device reporting and communications are not acceptable for Navy IDS system designs.

7.2.2.2 Point-to-Point. Communications conducted on one wire pair per device are point-to-point circuits. Typically, this circuit costs more to install than a loop system because of the additional wiring used to complete the system. One sensor to each of the circuits permits specific reporting by device and enhances the maintenance of the system. A single fault on the circuit disables only one sensor. Typical applications require low voltage wiring on 500 mA current or less wire, which is in pairs and which will require shielding if data is communicated (usually from control or data gathering units). This wiring scheme requires that the knowledgeable intruder bypass several diverse types and locations of wires in order to defeat the protection-in-depth schemes.

7.2.2.3 Multiplexed. Multiplexed is a term used to designate a communication technique that permits multiple communications on the same line to be differentiated and not interfere with each other. Usually more cost-effective because of the greater number of communicating units able to use the same pathway, the multiplexed scheme uses either frequency division multiplex or time division multiplex to separate the signals. Unique frequency or time designations are allotted to each reporting subsystem. The use of dual pair communications paths permits the loop to be maintained even in the event of one pair failure by allowing reverse of direction to continue communication on both sides of a fault. Multiplexing and demultiplexing equipment is a more costly technique than direct point wiring except where several devices could use the same pathway or loop. Frequently, access control systems provide up to eight multiplexed points for door alarms, etc. to be transmitted on the door control/reader lines as standard equipment. Multiplexed communications

are not to be confused with the party-line loop (McCulloh circuit) which are prone to cross talk and indecipherable message transmissions.

7.2.3 Telephone Line to On- or Off-Site. Very long alarm communication wiring can be managed by existing or specially installed telephone company wiring. Connections between buildings and within large facilities often can be cost-effectively accommodated by the telephone utility wiring, since most IDS communications needs are conducted via low-voltage wire pairs. Lease and installation costs, physical protection of wire routes, expansion capabilities, and availability of services are a few of the major considerations in comparing telephone facilities to proprietary wiring. Responsibility for maintenance can also be a problem. Caution must be observed on installations within air return plenum ceilings, which must be explicitly noted for conduit or plenum cable applications as required by local and national electrical codes and fire regulations. Various communications techniques can effectively extend the IDS information communications to points which are limited only by location of telephone communications instrumentation. These may include international satellite communications systems.

7.2.4 Radio Frequency. Radio frequency (RF) communication techniques may be used for IDS information transfer. Although most often used for two-way voice communications, there have been significant new developments in the RF alarm transmitter subsystems within the past 10 years. The primary use of RF alarm transmissions has been to provide for mobile duress alarms and for an inexpensive method for alarm signalling where wiring applications are impractical due to remote locations. "Wireless" systems work in conjunction with detection sensors to provide transmissions of the detected event from the device location to the monitor location. The signal codes permit separation of reporting for one to 10,000 distinct alarm reporting transmitters. Extreme caution should be exercised when using this type of device since transmissions are affected by interference (electric circuit transients, motors, transformers, ignitions, heating, static, weather, and other radio frequency signals). The output and power regulations of the RF devices must be licensed by the Federal Communications Commission (FCC). Long distances are possible through the use of signal repeaters and antenna systems, and methods of power supply or batteries require frequent supervision and maintenance.

7.2.5 Microwave. Microwave transmissions are extremely short radio waves. The microwave usage differs from radio frequency transmissions because on/off pulses rather than varying frequency are indicative of information. This differentiation permits high-speed information transfer rates for data, television signal, multiplexed telephone, and multiplexed alarm signals. Microwave is limited to line-of-sight transmitter to receiver (or reflector), behaves very much the same as light signals, and will not pass through buildings, trees or hills. There are very few atmospheric influences on microwave, and the system withstands adverse weather conditions. Systems are licensed through the FCC for IDS alarm and assessment (CCTV) equipment. The system designer may wish to explore the cost benefits of microwave data and video links, particularly in large or complex sites where cabling costs are

excessive and/or telephone lines are unreliable. Recent advancements in this technology offer potential advantages in security system communications.

7.2.6 Fiber Optics. High security IDS data transmissions are increasingly conducted via fiber optic cable. Data transfer on fiber optic cable is immune to electrical influences, static electricity, lightning, water, and EMI/EMR. Cable distances can be unlimited with the addition of repeater units. Protection against surreptitious compromise is inherent due to the sophistication of techniques required to monitor and compromise the signals and the apparent loss of signal when the line is bent or cut. Justification for fiber optic transmission techniques can be made using the following table if noted that the approximate costs are similar.

Table 16

Protective Techniques
for Alarm Communication Links

PROTECTIVE TECHNIQUES	COMMENTS	ATTACK TECHNIQUES	LEVEL OF SECURITY
BURY THE CABLE		DIGGING WOULD BE NECESSARY	LOW TO MODERATE
BURY THE CABLE IN CONCRETE		POWER TOOLS NECESSARY	MODERATE
FIBER OPTICS	BURIAL MAY BE DESIRABLE	POSSIBLY THE MOST SOPHISTICATED ATTACK WITH EXOTIC TOOLS	HIGH
ELECTRET CABLE	MUST BE BURIED	POSSIBLY THE MOST SOPHISTICATED ATTACK	

7.3 Remote (Control) Units. Remote or control units are essentially junctions for portions of the intrusion detection system that provide regulated power sources, distribution of communication, and sensor data collection capabilities. A typical remote (control) unit is depicted in Figure 44. Commercial products may be termed: data gathering units, transponders, field communications, master or slave, auditors, and data

concentrators. These units can also be used for local (area) reporting within the distributed IDS network. Communication wiring for these units requires sensor wiring usually two pair (or less) of unshielded direct current low-voltage cable or of shielded data communication pairs. The gauge and length of wiring specification is dependent upon system specific needs, often a limitation of wire resistance. Table 17 lists possible gauge and line lengths to maintain 30 ohms or less of resistance, normal parameter for an IDS line. The data communications line length and gauge is likely to be specified by the manufacturer for performance at a site specific installation. Care

Figure 44
Remote (Control) Unit

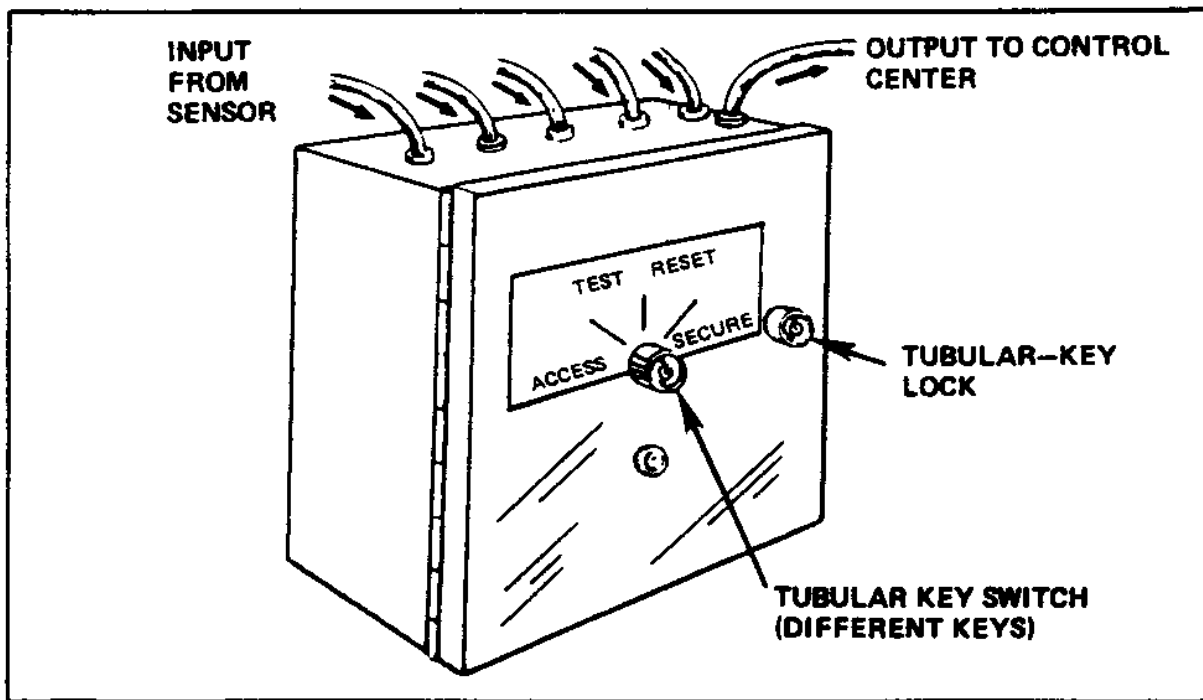


Table 17
Typical Alarm Loop Lengths

Wire Gauge (AWG)	Resistance (ohms) Per Kilo Foot	Maximum Loop Per 30 ohms
22	16.704	1795 ft
20	10.35	2809 ft
18	6.51	4608 ft

14	2.575	11,650 ft
Notes: 1. Resistance is measured at 77deg.F (25deg.C) 2. Loop resistance excludes end-of-line resistance (loop is total length of wire out and back)		

13.02-110

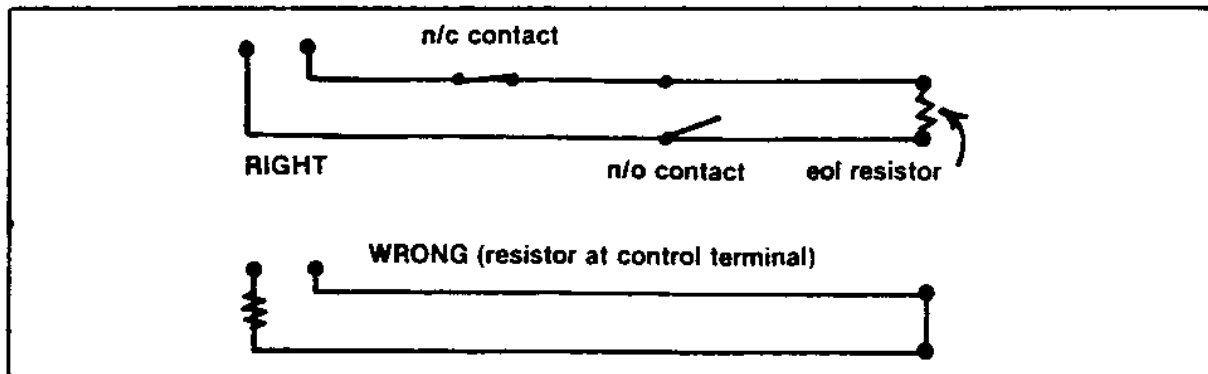
should be exercised when the communication line is adjacent to or crossing all other electrical, electromechanical, and electronic system networks. Degradation of signal, except for fiber optics, is possible from any static or electrical "noise." Figure 43 and Table 15 depict the relationship of the resistance of hardwire cable lengths versus size (thickness) for assessment communications applications.

7.4 Line Security Techniques. The importance of the Alarm Communications Network requires protection of this information from compromise. Planned or spurious violations of the complex wire lines require both specific annunciation and physical safeguards to ensure the accuracy of this extremely vulnerable network. The following paragraphs provide the criteria and concerns for amelioration of this vulnerability. Avoid systems which permit alarms to be shunted or ignored when using the access mode. It is better to have masking techniques that permit trouble or supervision alarms even when the system is in an unarmed state.

7.4.1 Line Supervision. Line supervision is the term used to describe the various techniques that are designed to detect or inhibit manipulations of communication networks. Detection of line compromise can be accomplished in a direct current circuit for open, short, ground, or foreign voltage by using a circuit resistance system as noted in Figures 45 through 49. Line supervision techniques are required for the protection of information pathways. Either active or passive methods are employed to detect the compromise attempts. Examples of detection methods include: use of modulated frequencies for information transfer, pulses and encryption techniques, polling schemes, and lack of information presence.

7.4.2 Physical Protection of System Components. Physical protection techniques are used to protect wiring exposed to physical damage and manipulation or tampering. The general method of accomplishing this protection is providing conduit or metallic tubing to accommodate wiring. This serves to protect wiring from: physical manipulation by unauthorized persons, chewing damage by rodents and, to a lesser degree, some fire protection and improvement of shielding characteristics. Tamper detection sensors are required on all junction boxes. The conduit connections should be tight, workmanlike, and free from mechanical defects. Exterior conduit should

Figure 45
End-of-Line (EOL) Circuit Design



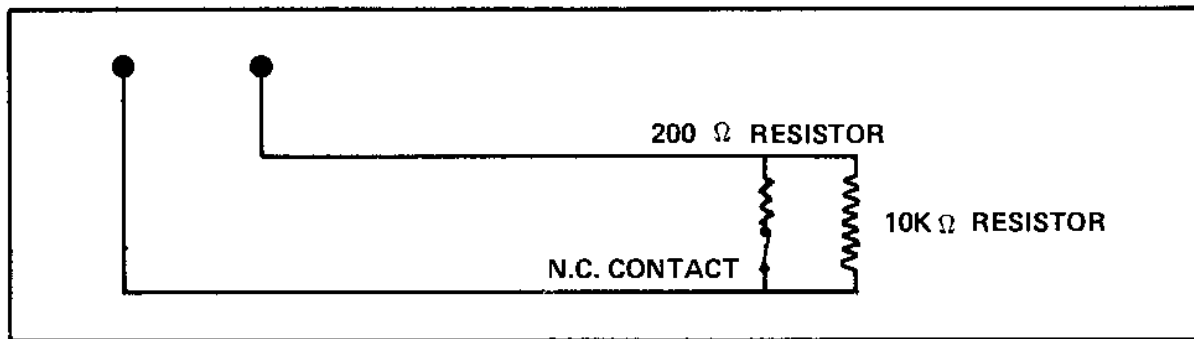


Figure 46
Dual EOL Resistance Circuit Design

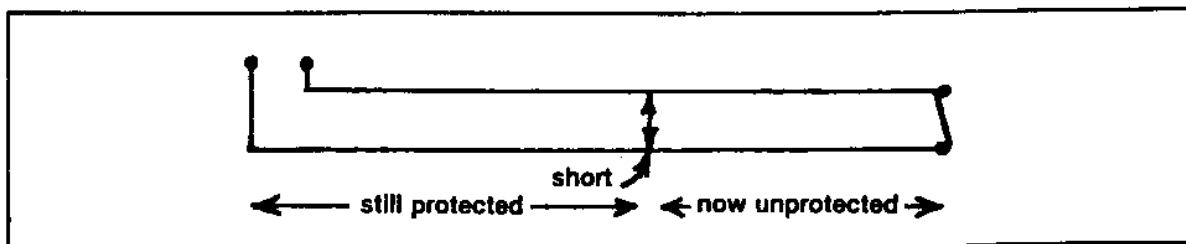


Figure 47
Short Occurring on "Hot Loop" Design

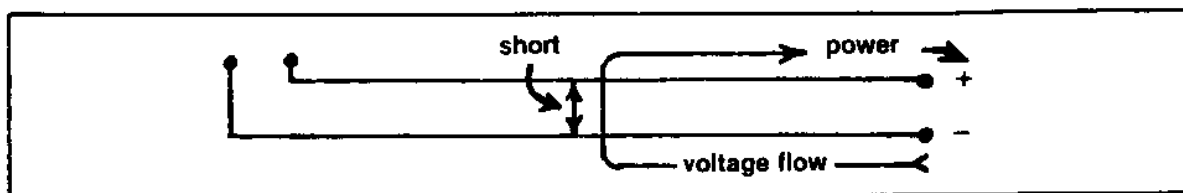


Figure 48
Short Occurring on "End-of-Line" or "Return Circuit Design"

Occurring on "Hot Loop" Design and Figure 48 Short Occurring on "End-of-Line" or

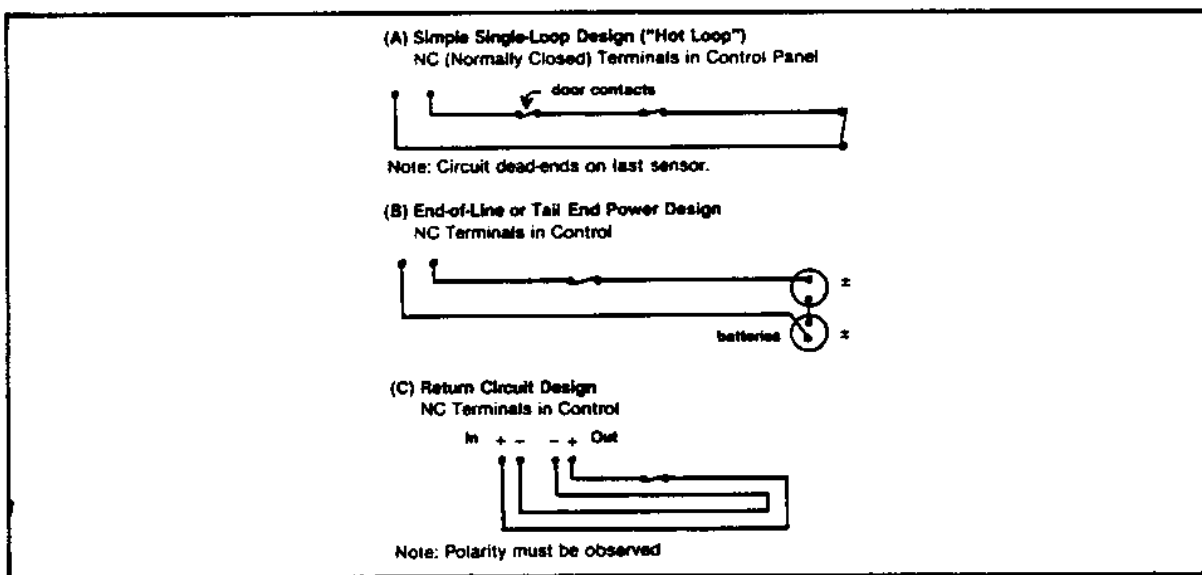


Figure 49
Protected Circuits

have connectors approved for that environmental application. In high security applications, the use of dedicated conduit pathways is recommended for IDS communication networks. Where possible, shared conduit systems can be used, although some care in mixing communication, sensor, and other data should be exercised to preclude "crosstalk" or interference. Conduit systems should be provided for a 25 percent expansion capability and the addition of a pull string (cable) within the network after wiring is installed. Compromising emanations and inductive coupling can be controlled by use of conduit and maintaining critical electronic components with the protective perimeter. Metallic conduit must be decoupled (insert of nonmetallic conduit) when exiting Sensitive Compartmented Information Facility (SCIF) areas to avoid fortuitous conductor conditions.

7.4.3 Environmentally Generated Interference. The environment of IDS components is comprised of influences which may be detrimental to proper system operation. Issues which affect all systems include primary and back-up power sources, electromagnetic interference (EMI), lightning and static, and other environmental considerations. The reader is referred in general to the NAVFAC Design Manual Series DM-4, Electrical Engineering.

7.4.3.1 Power Considerations. The electronic components of IDS rely on low voltage alternating or direct current circuits which are usually supported by battery modules capable of providing minimum operating time in the event of primary power source failure. This minimum back-up time is 4 hours. Care to develop total electrical load for generator and uninterruptible power supply use will control any variation in power which causes unacceptable performance of IDS components. The load should include 105 percent of full capacity of

the system with consideration of 5 percent of sensors in the alarm mode. Criteria for configuration of power supply includes: load requirement, critical load and expansion; continuous or intermittent outputs; protection time limits; distribution networks and attendant line losses; national and local electrical code requirements; and other criteria developed by NAVFAC DM-4.3, Electrical Engineering, Switchgear and Relaying.

7.4.3.2 Electromagnetic Interference (EMI). Interference can be introduced to unprotected IDS communication lines that are in close proximity to high voltage power distribution networks, large transformers, unsuppressed electric motors, and other communication techniques and systems. Protection from EMI/EMR includes avoiding the sources of the interference and shielding wire lines by means of specialty wiring (coax, foil shielded pairs, and metal sheathed cables), metallic conduit systems, and physical separation of power and signal systems. Criteria for EMI/EMR protection for wire communications is contained in NAVFAC DM-4.07, Electrical Engineering, Wire Communication and Signal Systems.

7.4.3.3 Lightning and Static. Destructive power surges from lightning and static can affect the complex IDS network of electrical conductors and electronic terminal devices (both detectors/sensors and control equipment). Safeguards from lightning, static, and power line transients should be initiated. NAVFAC DM-4.06, Electrical Engineering, Lightning and Cathodic Protection, develops the criteria for this subject.

7.4.3.4 Other Environmental Considerations. The IDS components and networks are influenced by many factors which affect the performance of the system. Care and protection of devices and wiring will involve periodic maintenance and possibly some esoteric protection measures. Examples of environmental influences include hurricane, rain, thunderstorm, snow, sleet, tornadoes, high wind and other severe weather; smoke, dust, sand, humidity, floods, high and low temperature, salt fog; and radiological exposure incidents. There are many factors that may affect the system, and the variables should be examined in order to implement the system in the most cost-effective manner for the Government.

Section 8: ALARM REPORTING AND DISPLAY

8.1 Intrusion Detection System Integration. The focal point of IDS integration is at the alarm reporting and display location. Regardless of the sophistication of the total system employed for facility protection (from a simple local annunciator to a complex computerized display console), all of the devices installed for remote detection, access control assessment, and communication need to be terminated at a control point for human interface and response. In many applications involving multiple protected areas within a facility complex, the control network will be comprised of a variety of local control units to gather communications from card readers for access, alarm points for detection, and CCTV for assessment, and transmit this data to a central console for command, control, and communications with on- and/or off-site security response resources. Much of the state-of-the-art commercial technology currently on-line has been developed with these centralized control functions as cost-effective requirements. While this manual does not propose the integration of ancillary functions such as energy management and equipment monitoring, Figure 50 displays the range of applications currently available. The remainder of this section will discuss the basic issues, options, and elements involved in this critical integration point of alarm reporting and display.

8.2 Locating the Alarm Control Function. Many factors will influence the decision of where to locate the intrusion detection system (IDS) alarm control center. The vital nature of the knowledge of alarm events require that the functions be protected from both natural disaster and physical attack. These considerations of protection should be implemented following a complete assessment of the vulnerabilities and requirements of the facility and activity.

8.2.1 Threat Considerations. The degree of threat associated to the IDS control system is considered to be as high as the highest identified threat to any portion of the facility. This high degree of concern is a result of the requirement to identify unauthorized intrusions and the probability of failure in meeting this requirement if the alarm report processing system is violated. The control center operations are considered to be vulnerable from both insider and outsider attacks and the principal vulnerability of the communication of event and alarm reporting which serves to provide information for response and resolution to detected intrusions. These apparent vulnerabilities can be diminished by using diverse termination schemes, physical protection countermeasures at the control facility, and duplicate control facilities (a primary and secondary control center with fully redundant systems). Physical site restrictions and budgetary considerations will also be major influences in the implementation of an operationally sound and cost-effective control center.

8.2.2 Termination Options. Table 18 lists choices of the general categories for reporting schemes. Each of the following options may be more effective when combined with one or more of the other methods.

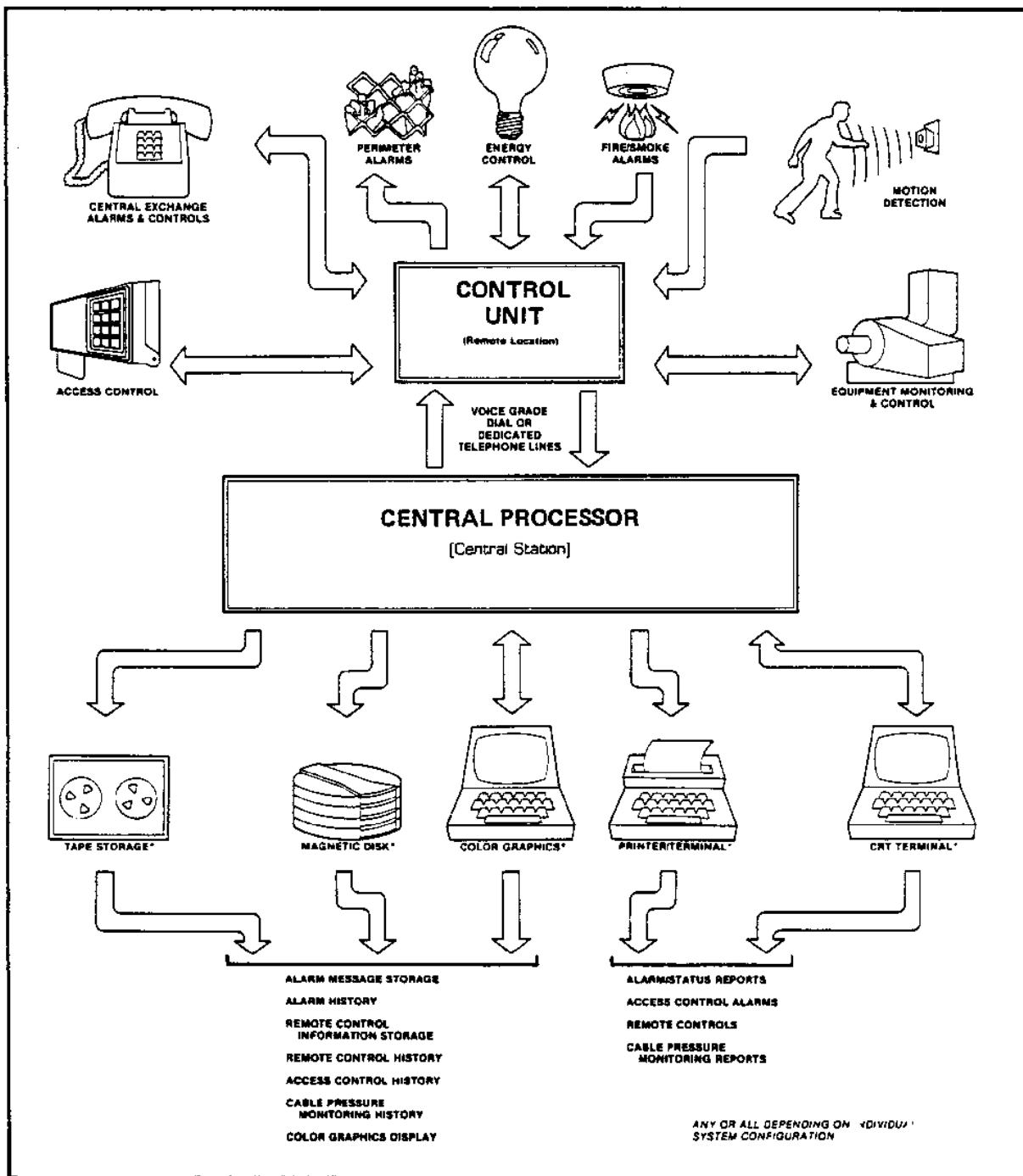


Figure 50
Integrated Facility Control System

8.2.2.1 Local. Local termination refers to the scheme of alarm reporting which provides very limited separation of alarm reports. The reporting device is usually a bell or siren mounted on the building exterior to provide indication of alarm related to the whole facility. The advantage of this type of report is that attention is directed to the place of alarm and the intruder knows that a detection has been sensed. The disadvantage of this system is in the simplicity of the physical attack needed to disable the reporting device and the reliability of depending upon others for report communications. This is a low threat, minimum security option.

8.2.2.2 Central Station. The central station termination scheme is a reporting option which uses a shared monitoring service. The typical system configuration consists of a premise alarm reporting from one to several coded alarm conditions to a monitoring receiver normally via a dial telephone network. The monitoring personnel (who are typically monitoring other subscribers concurrently) then inform authorities or responding forces of the location and type of alarm event. This information is limited to the detail of separation in alarm zones at the facility. Historical records kept by the central station may be of limited value in reconstruction of events reported by the premise alarm system. Various levels of Central Station security coverage are available and should be keyed to the threat requirements.

Table 18
Alarm System Termination Options

- LOCAL
- CENTRAL STATION
- POLICE DEPARTMENT
- PROPRIETARY

8.2.2.3 Police Connection. This connection is similar to the shared service option except that the reports are monitored directly by the responding forces. The leased line connection which characterizes this type

of reporting permits a line security technique to assure proper operation of the system report capability. The major disadvantage of the police connection and central station options are the vulnerabilities of the required telephone facilities. Also, many municipal police departments are discontinuing these services due to nuisance alarm response requirements and higher priorities on calls for service.

8.2.2.4 Proprietary. The proprietary termination option indicates the use of an intrafacility protection scheme which relies on monitoring and response personnel dedicated to the facility. This scheme permits a greater definition of alarm zones since wiring of point-to-point devices is much easier than most shared service schemes. The goal is to have detectors provide an individual report per detection device. The improved characteristics of information quantity, supervision of communication lines, and processing capability demand the presence of proprietary personnel to coordinate the response forces and provide for additional resources as required to resolve the problem. This is the preferred method for DoD facilities and is the method required by OPNAVINST 5530.14, U.S. Navy Physical Security Manual, for all Navy facilities.

8.2.3 On-Site Location. Considerations for locating a control center on-site include provisions for personnel, equipment, and procedures. The decision is influenced by the threat analysis conclusions that indicate the need for immediate response and resolution of alarm and event reports. High value assets, mission criticality, remote location, directive requirements and budgetary constraints are a few factors which indicate a proprietary or on-site control center. The decision to provide a local on-site control center for alarm processing will realize immediate response capability when communications and priority controls are implemented. The trade-off for in-house controls is the vulnerability of the control center itself. In order to adequately address the vulnerability of the control center, it is necessary to critically examine the need to provide this high level of security.

8.2.3.1 Personnel. The vulnerabilities of personnel to physical attack and compromise of duties are diminished by protecting the control center to the same degree as the highest security application within the facility. Comprehensive access control serves to eliminate unauthorized personnel from the center, thus avoiding distractions and compromise of security tasks. Although there are some cost savings and subdued image merits to the open, "receptionist" type security control center, the mission of the security forces is better suited to the protection afforded by a location that is out of public access. Physical protection of the control center begins with the limitation of public view, particularly from outside the protected perimeter; fire detection and extinguishing equipment; duress alarms (reporting to an off-site response force); physical (brute force) attack protection; bullet-resistive materials; and centralized assessment and communication systems. Comfort provisions include items which will enhance the ability for monitoring personnel to conduct duties with the minimum of outside influences. These considerations include heat, light, air-conditioning, toilet facilities, human factored equipment and work areas, and appropriate training. Adequate staffing will provide for the proper rotation, scheduling, and relief to ensure reliability and effectiveness of personnel.

8.2.3.2 Equipment. The equipment used for the on-site control center also requires protection and comfort considerations similar to those noted for personnel. The critical nature and vulnerability of intrusion detection systems (IDS) indicate a need to protect the communication components of IDS-on-site equipment which should include point-for-point alarm zoning regardless of the control center location. This will enhance reliability and specificity of information and maintenance. The problem of having a block or area of alarms inoperative due to a single point failure is then moot. Physical characteristics of the utilized equipment will indicate the need for considerations of environmental influences. The physical location of the control equipment should be within the protection of the alarm system perimeter and protected to the highest degree of security encompassed by the system. Equipment sensitivity to heat, cold, humidity, moisture, dust, static electricity, radio frequency interference, electromagnetic interference, and power fluctuations will require particular support systems to control or eliminate these influences. Systems may provide inconsistent operation if designated operating conditions are not met. Specifications listed on equipment catalog sheets will provide insight to the environmental needs of equipment, and manufacturer's or engineering support will have resources to document and provide support requirements for environmental considerations peculiar to the specific equipment. Since the primary goal of the on-site installation is to provide information of alarm conditions for assessment and response, care should be taken to have valid and reliable output in a consistent and clear format. Communication of events to secondary reporting centers and additional response forces may be considered for facilities which require back-up security coverage or special materials handling for safety. Regular scheduled preventive maintenance and testing are also required to ensure proper operation.

8.2.4 Off-Site Location. The decision to locate the control center away from the protected facility is primarily influenced by: 1) the ability to define regular duty and off-duty hours and to complete a secure facility during nonduty hours; 2) lack of appropriate resources for a control center; 3) limitations that inhibit deployment of on-site response personnel; 4) duplication of report communications due to higher security needs; and 5) budget constraints which require consolidation of resources.

8.2.4.1 Personnel. The ability to provide trained personnel to respond to alarm events is often better addressed by a law enforcement organization organized specifically for this task. These forces are necessary when manning of the facility is cost prohibitive or the outside forces are needed to augment the on-site contingent. If the facility can be secured with appropriate devices and physical response requirements can be met, then it may be more effective to provide an off-site control center. Caution is advised in permitting off-site forces to cover too many facilities with too few resources which generally do not consider the vulnerability of a facility with the same specificity as the activity. Off-site personnel are best suited to respond to given situations only if adequate information and direction can be given either by specific, point-for-point alarm information or in a backup role to on-site personnel.

8.2.4.2 Equipment. An off-site control center requires the same point-for-point alarm devices at the protected premise, but changes in control and communication equipment are necessary. The control equipment will consist of two controlling elements: the premise controller, which provides status reporting (on, off, trouble, and alarms) and standby emergency power for alarm devices, and the reception station which annunciates specific status reports to provide the information required by off-site response personnel. These communications techniques are one-time additions to the security system cost that are contrasted by the recurring expense of personnel and training costs borne in the shared system budget. The transmission techniques detailed in Section 7 are utilized for this communication of information. Choice of technique (influenced by existing shared system) will dictate equipment considerations for the premise.

8.2.4.3 Procedures. The use of off-site responding personnel limits the complex and diverse results of event reports and alarms apparent with in-house resources to clear, concise and consistent actions. These action-oriented resolutions by responding personnel provide effective security at the expense of imposing restrictions on facility uses that are out of the ordinary. Specific information and concise response will provide efficient solutions to the problem. Procedures of apprehension are likely to be primary goals of the off-site personnel in contrast to the objectives of on-site personnel, which are to assess alarms and minimize asset loss.

8.2.5 Redundancy Considerations. The protective function of security control center implementation may require the additional safeguard of redundant reporting and display. This redundancy may be accomplished in a scheme similar to Figure 51. This figure depicts a redundant reporting system consisting of detection devices reporting to both local annunciation and an

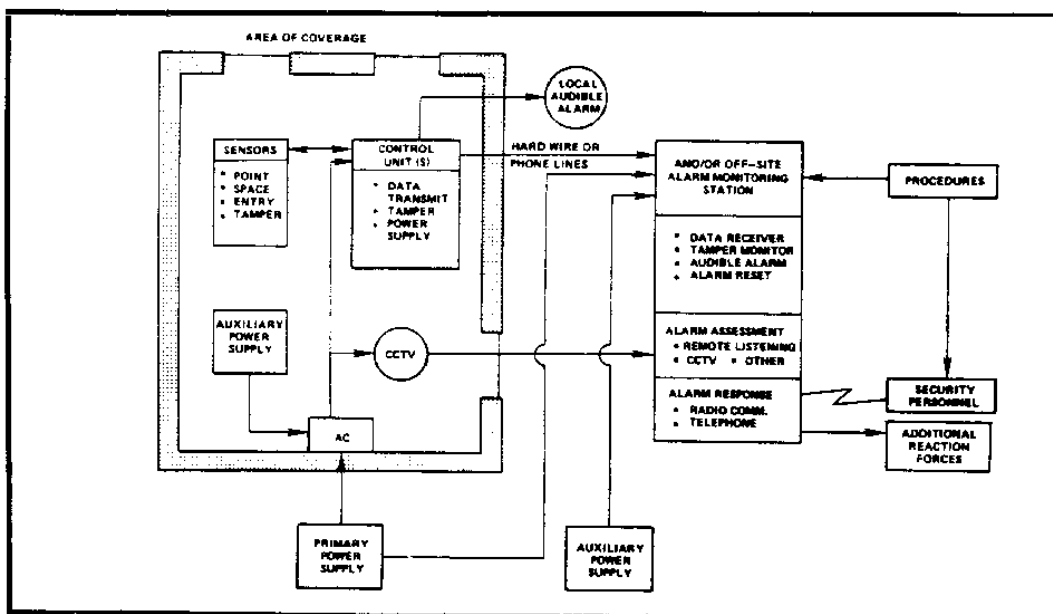


Figure 51
Relationship of the IDS Alarm Reporting and Display
Function to Other Security System Components

off-site alarm monitoring with local security personnel response and additional reaction forces. Redundancy in high security applications would require a primary alarm station on-site with an off-site duplicate for backup. Theoretically, this model could duplicate each reporting and display function such that any single point failure would not inhibit the system functioning. Safeguards to system operation include some consideration of redundancy at the component level. These concerns include maintenance of backup copies of system software and on-site storage of point sensors or components critical to system operation. Duplicate pathways of communications are also to be considered.

8.2.5.1 Control Center Configuration. The control center operator is the focal point of command, control, and communications for facility security operations. Distraction, disruptions, and discomforts which impact these operations need to be controlled in order to prevent control failure. Since the operator is responsible for monitoring and dispatch functions, which are essential to the safeguards of the facility, it is important to maximize the physical and visual access to the display and maintain a limit of outside access by nonauthorized outsiders.

8.2.5.2 Human Engineering. The purpose of human engineering is to avoid operator fatigue, to maximize operator efficiency, and to control and eliminate consequent operator errors. The environmental conditions of the control center, i.e., temperature, humidity, ventilation, noise, and light, should all be at optimum. The workspace should be designed to accommodate and enhance operator functions. Complete assessment of items the operator must see, manipulate, and hear will indicate the requirements for the console design. This listing will be prioritized to permit both routine and exigent tasks to be accomplished in a logical manner. The following suggests the comfort conditions of the workspace area and console design: temperature (65 to 75 degrees F; humidity (30 to 70 percent); ventilation (13 to 20 cubic feet per minute); noise 0 to 85 decibels, avoiding continued silence); and light 20 to 100 foot-candles, avoiding glare and surface reflection). Competing priorities for control layout should favor visual tasks of the console/display function, controls which interact with visual tasks, and emergency controls, anticipated sequence of operation (from left to right and top to bottom), convenience layout according to frequency of use, and consistent design to other systems in descending order of priority. Refer to Military Standard Mil. Std. 1472B, Human Engineering Guide for Military Systems, Equipment and Facilities for detailed descriptions of console and workspace layout. Nuclear Regulatory Commission and Sandia Labs documentation is also instructive in these critical areas.

8.2.5.3 Physical Security. The control center is the single most vulnerable point of the intrusion detection system due to the concentration of alarm reporting and dispatch function in this area. These functions should be protected to at least the same degree of security afforded to the most valuable asset within the facility.

8.3 Using Existing Equipment. When upgrading the IDS for a facility, significant savings can be realized if existing equipment can be used. The

measure of value to this reuse project comes from a comparison of how well the current system serves to counter the vulnerabilities identified in the threat analysis. The problem of integration arises when various sensors are grouped into the electronic operating network. The sensor installation and operation must be examined carefully to determine the relationship of each device within the system. The advantages of integrating a variety of sensors are realized in both cost savings and improved protection if system engineering is done carefully. The engineering task is critical when the control system and reporting/display terminations are designed. Existing older control equipment is less likely to fulfill the requirements of an integrated design due to the lack of expansion capabilities. Although caution is advised, compatible existing equipment from reputable manufacturers can be used in updating the control system. Where care is taken to design-in newer elements consistent with user effectiveness, given the advent of microprocessor technology and state-of-the-art display, reduced control systems costs may result in replacement of older networks with the increased capabilities of the new.

8.4 Reporting and Display System Components. The reporting and display systems are roughly categorized as follows. These termination options offer advantages and disadvantages as noted previously. The techniques of reporting the system detections are indicative of the presentation and transmission of information. Obviously, the amount of information processed and displayed increases the cost.

8.4.1 Annunciator Units. Annunciation of alarm signals are presented by visual and audible indicators which relate to the on/off nature of detection sensors. Either or both visual and audible indicators are used within a particular transmission technique that meets the requirements of the receiving and display system.

8.4.1.1 Modular Single Point Alarm Displays. The technique of alarm reporting requires that the sensors within a zone are looped to report any detection on the loop. Typically, this scheme provides visual and audible indications of alarm conditions. The modular capabilities of this type of device provide limited expansion in groups of four to 10 sensor zones. The line security for this type of system is often not present when not in the armed state. Generally, detection loop length is a short (under 500 feet), two-wire type on which direct current is also passed. Open or short circuits are indicative of trouble or alarm. This feature and the "daisy chain" approach to expansion often defeats the cost-effective benefit by impeding maintenance of systems.

8.4.1.2 Digital Receiving Devices. Digital receiving devices are used for centralized reporting of alarm conditions. Individual transmitting devices report a limited number of signals (less than 10) with a system specific code number. This system is used in central station and multiple premise proprietary systems due to the availability of reporting on voice grade (dial) telephone networks. Upon activation of an alarm device, a microprocessor circuit initiates a telephone line securing process, dials a telephone number, identifies itself, and indicates the zone of alarm. The system of

communication is inexpensive and relatively speedy. The advantage of this type of installation exists where leased telephone line pair or proprietary wire connections are impractical due to unavailability, extreme distances, or high cost. The disadvantage is in the limited (less than 10) number of reporting zones per system and the vulnerability of the telephone line used for reporting. The principal applications of the digital reporting scheme is residence and retail establishment usage in the central station or police connect terminations.

8.4.1.3 Simple Multiplexed Alarm Reporting Systems. Multiplex alarm reporting is a relatively new technique capable of having several simultaneous reports use the same circuit. Differentiations in time or frequency separate the individual reports to avoid interference or clashing which would result in incomprehensible messages. The system requires the signal to be separated (demultiplexed) at the receiving end in order to display and record the event reports. Multiplex wiring advantages are apparent where multiple reports on the same circuits are required, such as in large systems where one pathway could be used or multiple reporting premises have large reporting needs (up to 256 sensor zones per subscriber). The same is true where very high point-to-point wiring expense is evident and line supervision polling techniques are required for security. The disadvantage is the vulnerability of reports beyond any fault in the line and costs of telephone facilities, engineering, and receiving equipment.

8.4.1.4 Microprocessor-Based Alarm Reporting Systems. The equipment for this system requires point-to-point wiring, and the display is initiated on an "IF - THEN" scheme. Audible, visual, and language annunciation can be used in local or remote centralized reporting. The transmission techniques can be individual dedicated wire pairs for each display terminal or digital, multiplexed communications. The most popular method of transmission is via modem because of the vast amount of information available through this system and the ability to provide control to, in addition to monitoring from, a remote site. The local reports of events and alarms must be changed into a transmittable form and translated at the central control. The modulation/demodulation technique is used commonly for the transfer of computer-to-computer information over existing telephone line facilities. The benefit of microprocessors with cathode ray tube (CRT) displays over other annunciation devices is the method of information display regarding the alarm or event reporting. When an alarm occurs, the device identifies the specific location (usually in English) of the occurrence and provides information regarding the proper course of action to follow. Decisions of "what to do next" are removed from the discretion and interpretation of the responding personnel by the previously determined directions associated with each event report. Figure 52 illustrates a microprocessor-based reporting and control system which incorporates multiplexed data path scheme. This system is appropriate for both exterior perimeter and individual facility applications and is in use at many Navy facilities.

8.4.2 Status Control. The status indications of the display system are divided into the annunciation of particular event reports. The need to clearly differentiate the indicators is apparent when the system size is

greater than one reporting device. Specific status is always relayed to individual zones of alarm.

8.4.2.1 Alarm. The status of alarm is indicated by visual and audible indicators in the event of a sensor detection of a violation. The visual representation of a red-colored light and an appropriate tone sounder or siren are the usual indicators. A steady light and tone normally indicates an intrusion alarm and an intermittent light and tone normally indicates a fire alarm. Careful differentiation of alarm indications should be made from other event reporting to call attention to the matter with the greatest urgency and clarity. Visual indicators are best for this purpose. Caution is advised in the use of differentiated audible tones for alarm annunciation as it has been proven to be unmanageable and confusing in systems requiring more than four specific tone annunciations.

8.4.2.2 Access. The indication and reporting of access refers to the condition where alarm devices are ignored due to an expected time or event related violation of detection devices. This violation must occur when a protected premise is entered. There are two methods which accomplish the access mode: shunting and masking. Shunting removes the reporting zone physically from the system by creating an open or short circuit in place of the alarm zone. The disadvantage of this technique is the loss of trouble reporting which creates a vulnerability to system maintenance during the shunt period. Masking is a technique which ignores only the alarm reporting and allows status of communication line to be maintained. Access conditions should be limited to the smallest number possible to avoid facility penetration during downtime and should be compensated for by procedures and additional security forces as required.

8.4.2.3 Trouble. The indication of trouble will only be present with systems sophisticated enough to provide this feature. Most systems (except for microprocessor based or computerized) rely on the obvious loss of communication or inhibit feature to indicate trouble. Trouble can be one or all, short, open, ground, or foreign voltage, i.e., any condition which inhibits the use of the report transmission facilities. Trouble indications require communications or current to be present on the line at all times. Interruptions or changes to the signal are the sense of trouble or line fault. Malfunctions and tampering are thus controlled by line supervision techniques.

8.4.2.4 Secure. This visual or audible signal is present when current or communication can be carried on the signal transmission facilities and the sensors are "armed." Some systems rely on the absence of secure indication to indicate trouble. Simple systems will have a "ready" or secure indicator to indicate closed loop status prior to arming the alarm circuits. This indication is very important to the proper maintenance of the intrusion detection system.

8.4.3 Hard Copy Output. Hard copy output refers to the alarm report indications that is in printed form. This printed information may be a simple

numeric sequence, alphabetic and numeric sequence, or English and other languages. The paper report is an invaluable resource for after-the-fact investigation and reconstruction of events.

8.4.3.1 Line Printer. The line printer is a high-speed computer peripheral that prints a line of text in a single burst and is capable of printing up to several hundred lines per minute. This information can be quite bulky when stored for later review. Line printer use for a security system is usually confined to historical report compilation which may burden an ordinary printer.

8.4.3.2 Other Printers. The usual report printer associated with a security system prints at a maximum speed of one line per second and accommodates 8 1/2-inch by 11-inch paper (or smaller) in continuous form. The least desirable of these types of printers are the roll or strip printers, an inexpensive item which limits line length to 16 characters or less, and which prints data that is difficult to file and reference. Information on the smaller printers is often in abbreviated or numerical form which is a compromise in comprehension due to cost.

8.4.4 Visual Reporting. The devices described below provide report information regarding alarm system monitoring and control functions. These devices usually provide an audible signal to draw attention to the display and permit silencing of the audible signal (see Figure 52).

8.4.4.1 Alphanumeric Arrays. The alphanumeric array is a display feature which consists of relatively simple coded information (three to 16 characters) which differentiates alarm zones. Best suited to extremely small applications, this device permits indications of alarms in an economy of space. The simplicity of this reporting system does not exhibit features of prioritization and line security techniques. This dot matrix, or light-emitting diode display system, is useful for two to four zone reporting functions.

8.4.4.2 Cathode Ray Tube (CRT) Displays. The CRT display is used to provide reports, operating copy, written copy, and graphic arrangements. The display element is often part of a video display terminal (VDT) that permits display and system control functions. Since the information that is reported is an output of a processor, there is often much more information available than in common point alarm indicators. Instructions to operating personnel based upon the series of detected events can also be displayed.

8.4.4.3 Graphic Displays. The video display terminal can also be used for presentation of graphic information, often in color. For alarm reporting systems, floor plans, site plans, and maps can be displayed in colors with conspicuous representation of zones and areas in alarm. Specific color schemes can be indicative of priority or emergency alarms and direct attention

to the represented areas with a minimum of training. Other types of graphic displays, particularly screen and slide systems, although relatively cheap and easily updated, very often fall prey to mechanical problems due to long periods of inactivity.

8.4.4.4 Light-Emitting Diode (LED) Displays. This small, bright lamp provides extremely high performance characteristics and basic colors for alarm reporting and display. The arrangement of LED displays is usually either in grid (tabular) or map (and combinations) format, and conventional acceptance of color relates red to alarm, green to secure, and amber to access. Trouble indications are reported either as blinking alarm or secure indicators. The most popular of these displays depicts the protected facility in outline graphic form on a wall map up to 40 inches by 80 inches in size. It provides three colored LEDs for each protected area, which permits monitoring personnel to easily direct response forces to the specific area of alarm and adjacent areas as new intrusions are detected.

8.4.4.5 Mobile Displays. The mobile display is an alarm annunciation device that can be remote from direct wire connection to the operating alarm system control center. The system uses microwave, radio frequency, or other transmission techniques to provide display information to the remote unit. Very popular items for large facilities requiring vehicular patrols, these devices indicate alarm information either with alphanumeric or map display indications. Particular remote alarmed zones can be responded to quickly, since information is automatically passed to the remote or mobile units.

8.4.4.6 Closed-Circuit Television (CCTV) Monitor Displays. The CCTV system may also be used for alarm display functions, particularly where immediate assessment of areas out of direct view of security personnel is required. These components can provide the view in response to alarm detection. Connections are required between an alarming video switcher and the IDS. CCTV images may also be used as an intrusion detection sensor if the change of image is indicative of intrusion. This motion or image detection is not reliable in views which change due to expected movement (i.e., windblown objects) or rapid changes in lighting or contrast (Section 4, paragraph titled "CCTV-Motion Detection").

8.5. Conclusions. Navy facilities housing critical assets where IDS is deemed appropriate will require comprehensive analysis, design, and system engineering to ensure effective integration of the range of countermeasures applicable to their unique security needs. Figure 53 provides a graphic example of how the various security subsystems are integrated at the command and control center for definitive response by the security organization.

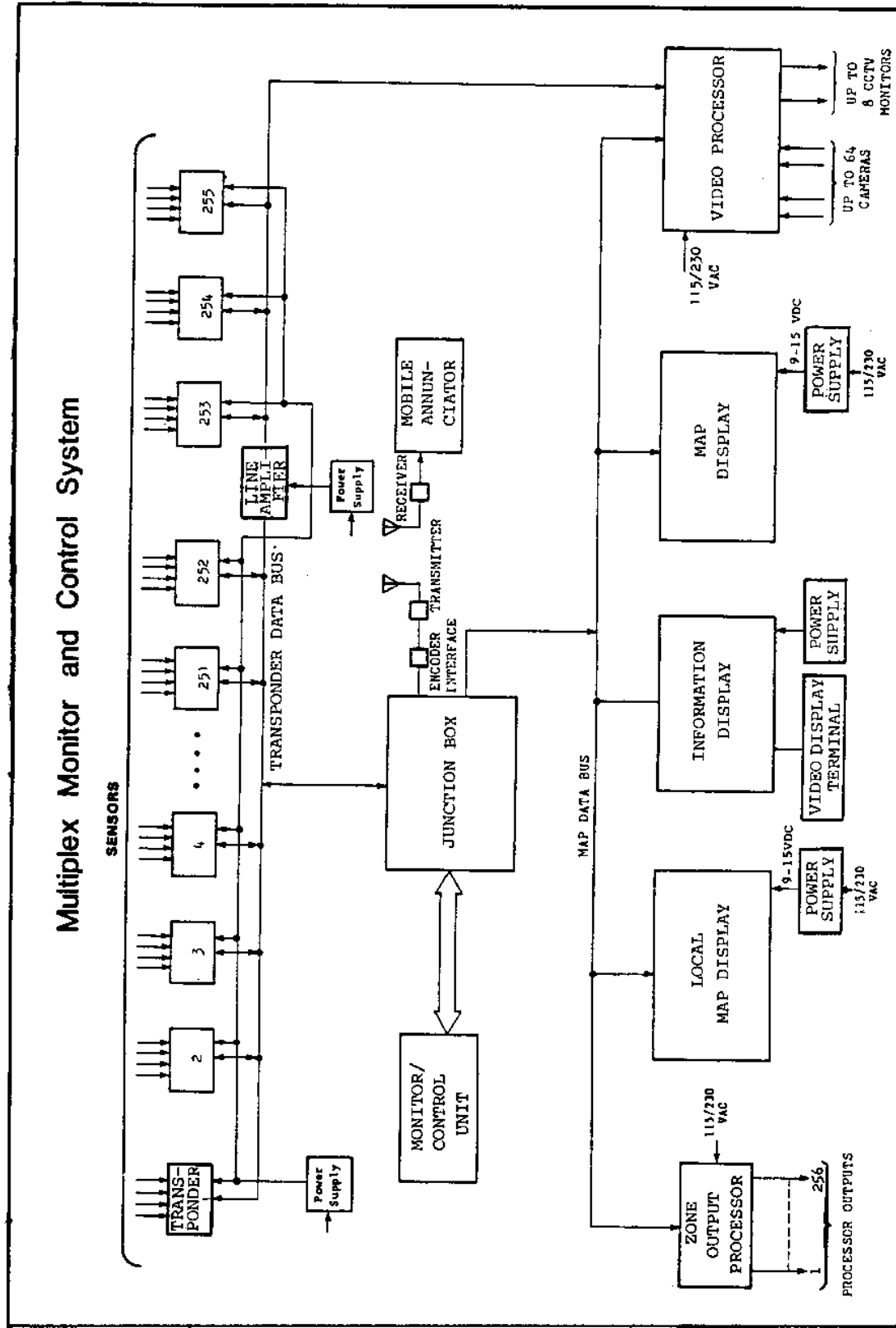


Figure 52
Microprocessor-Based Reporting and Control System

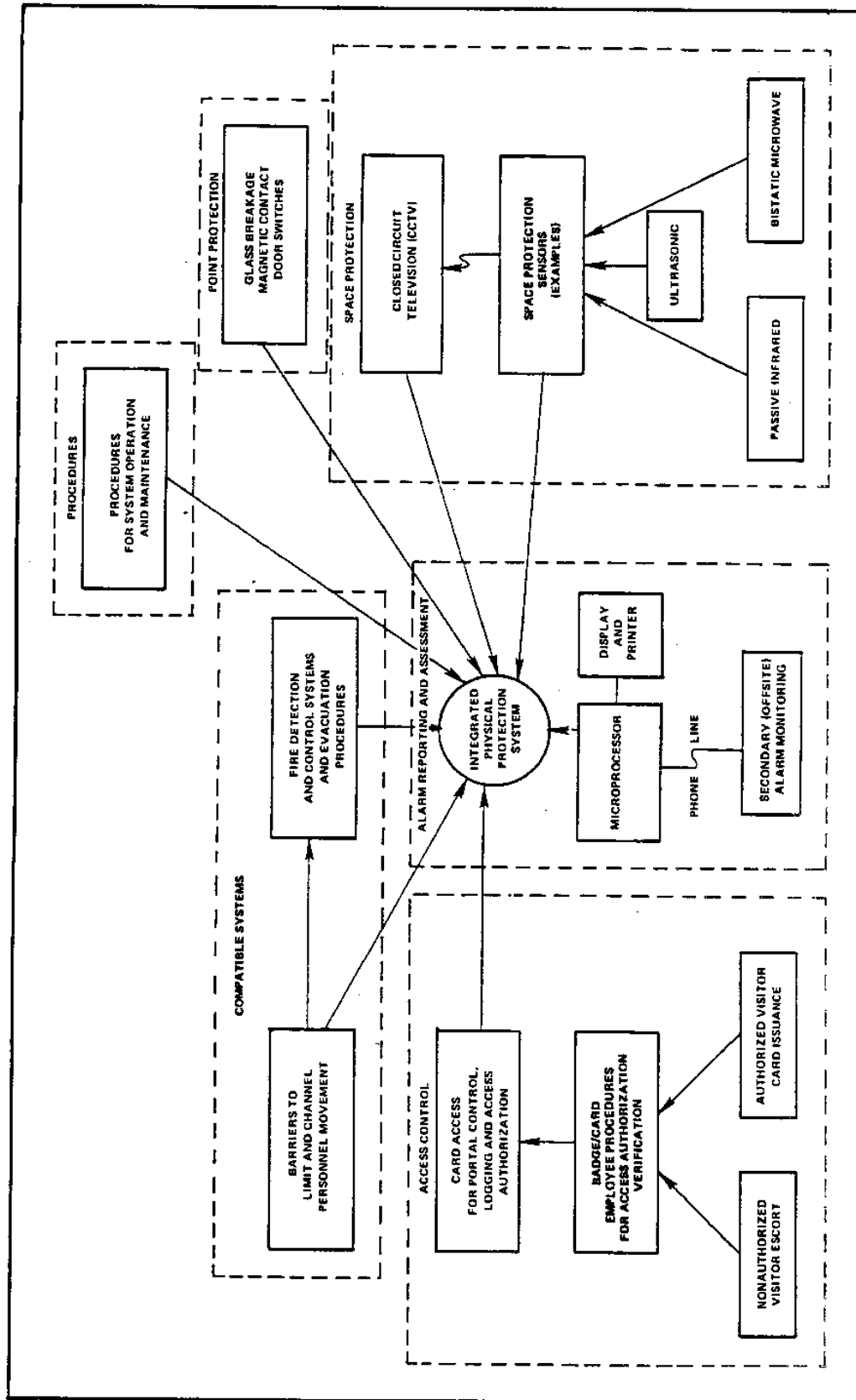


Figure 53
Integrated Physical Protection System

SECTION 9: POTENTIAL SYSTEM CONFIGURATIONS AT GENERIC NAVY FACILITIES

9.1 Introduction. The following pages consist of examples of intrusion detection systems application for generic Navy facilities. Each of these examples consist of a drawing with applied symbols and a brief written description of system operation. The examples are illustrations of placement of intrusion detection systems components and are not intended to be the only possible application for any specific facility or component. The examples are in the following order:

1. AIRCRAFT HANGAR
2. COMMUNICATIONS FACILITY (EXCLUSION AREA)
3. SUPPLY WAREHOUSE
4. FUNDS AND NEGOTIABLE INSTRUMENT STORAGE AREA
5. INTRUSION DETECTION SYSTEM MONITORING AREA
6. BX RETAIL AREA
7. COMMISSARY RETAIL AREA
8. COMMAND QUARTERS
9. SENSITIVE COMPARTMENTED INFORMATION FACILITY
10. NAVY AND MARINE CORPS RESERVE FACILITY
11. TRAINING FACILITY
12. AUTOMATED DATA PROCESSING FACILITY/AREAS

The following symbols are used throughout this section:












	=	CONTROLLED ACCESS POINT
	=	BALANCED MAGNETIC SWITCH
	=	AUDIBLE ANNUNCIATOR
	=	DURESS SWITCH
	=	INTERCOM STATION
	=	CLOSED-CIRCUIT TELEVISION MONITOR
	=	CLOSED-CIRCUIT TELEVISION CAMERA
	=	PASSIVE INFRARED MOTION DETECTOR
	=	LOCAL CONTROL/ANNUNCIATOR UNIT
	=	CONTROL UNIT
	=	ULTRASONIC

Figure 54
Sensor Symbols

9.2 Aircraft Hangar. This facility IDS is designed with perimeter and interior sensors reporting through a control unit to both a local audible annunciator and to a central monitoring point (Figure 55).

9.2.1 Perimeter. The perimeter IDS components consist of balanced magnetic switches, recess mounted, on all exterior connecting doors. Alarm devices will be armed for all hours when the building is not occupied.

9.2.2 Interior. High risk compartments and interior corridors are protected by passive infrared motion detectors. These sensors provide defense-in-depth and will permit compartmentalization by the system should only a small portion of the building require alarm devices protection with other contiguous areas open and available for use.

9.2.3 Alarm Reporting and Display. Independent zone controls will enable zones to be in access or secure modes at the same time. The control unit supervises all wiring for tamper even when the system is entirely in access. The status information is communicated to the central monitoring point via telephone links. A local audible annunciator alarm bell or siren will sound whenever an alarm occurs to provide both a local alerting capability to security patrols and a deterrent effect to an intruder attempting penetration.

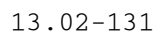


Figure 55
Aircraft Hangar

9.3 Communications Facility (Exclusion Area). This facility IDS consists of automated access control, detection, and assessment subsystems (Figure 56).

9.3.1 Automated Access Control. The automated access control subsystem will permit previously approved individuals to enter the Exclusion Area, specific offices, and other areas. This subsystem must not mask the intrusion detection device reports. The controlling, decision-making electronics are located within the protected Exclusion Area perimeter.

9.3.2 Detection. The detection subsystem consists of point and volumetric sensor components. The point sensors are balanced magnetic switches on portals which are outside the protected perimeter (approach hallways) at the protected perimeter (entry portals) and specific offices based upon assets contained within the rooms. The volumetric protection uses ultrasonic motion detectors outside the protected perimeter (approach hallways) and within the high security areas. The ultrasonic phenomenology was chosen because of the stable environment and the potential of heat-producing assets within the protected area voiding the effectiveness of passive infrared devices.

9.3.3 Assessment. The assessment subsystem supports the access control and detection subsystems by providing closed-circuit television (CCTV). Camera coverage provides assessment of alarms at vulnerable areas. The multiple entry points are effectively monitored by the minimum two guard personnel, thus more efficiently utilizing manpower. Exceptions to the access control and alarm system operation can be monitored and corrected by using the CCTV assessment system and an intercom.

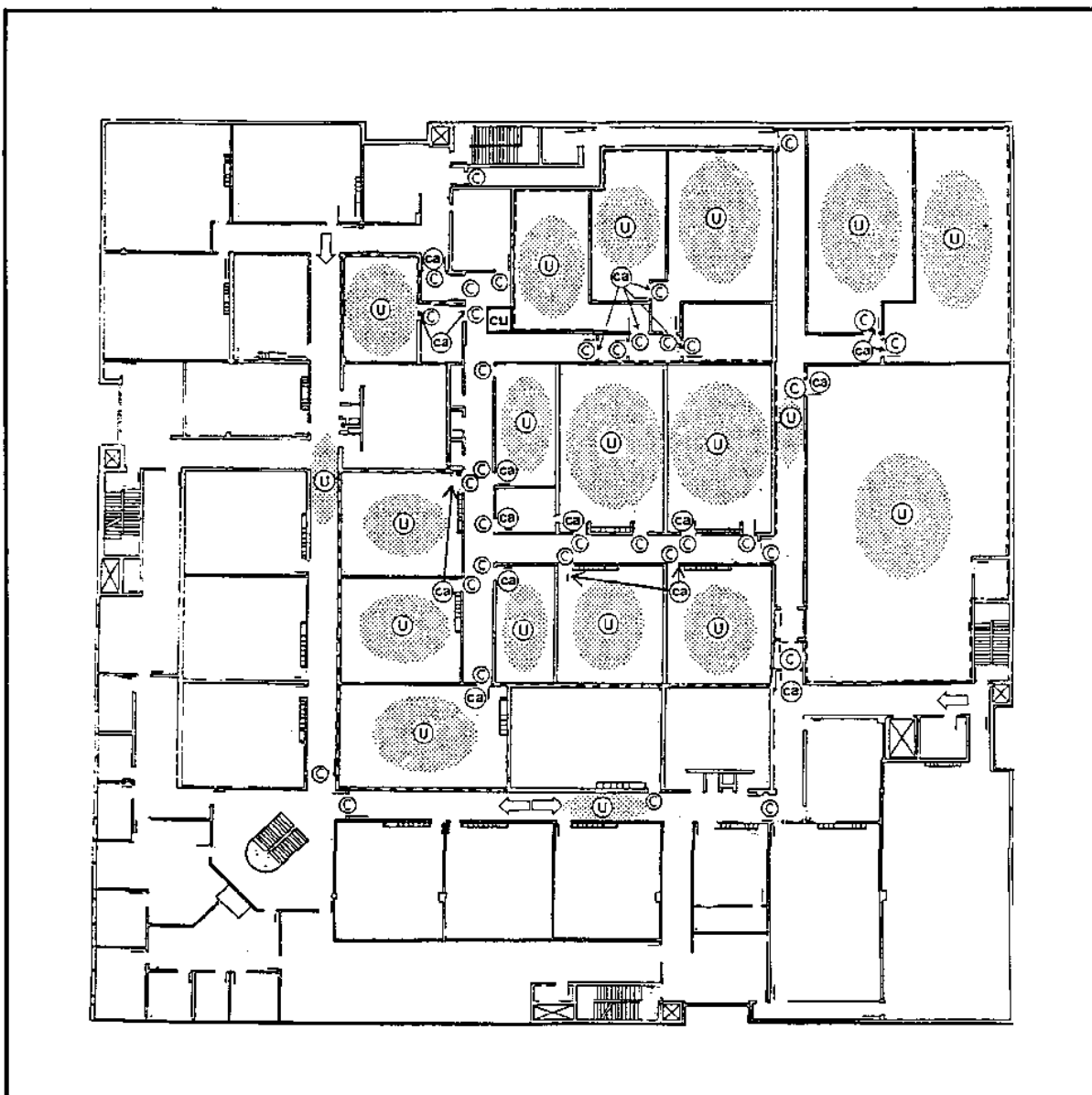


Figure 56
Communications Facility (Exclusion Area)

9.4 Supply Warehouse. This facility IDS consists of detection and assessment subsystems and an interface to a central alarm monitoring station (Figure 57).

9.4.1 Detection. The detection system consists of perimeter door balanced magnetic switches and interior volumetric motion detection sensors. These will report through a control unit to a local annunciator (siren or alarm bell) and a centralized alarm monitoring station. The use of the IDS to detect intrusion would be limited to after hours and when critical assets are stored within the facility.

9.4.2 Assessment. The assessment subsystem consists of closed-circuit television cameras continuously time lapse recording during all hours and keyed to the detection sensors to provide real-time recording of alarm events.

9.4.3 Control. Response to alarm events are reported to the off-site central alarm monitoring station (e.g., Base Police) through a control unit which also causes a local audible annunciator to sound when an alarm occurs.

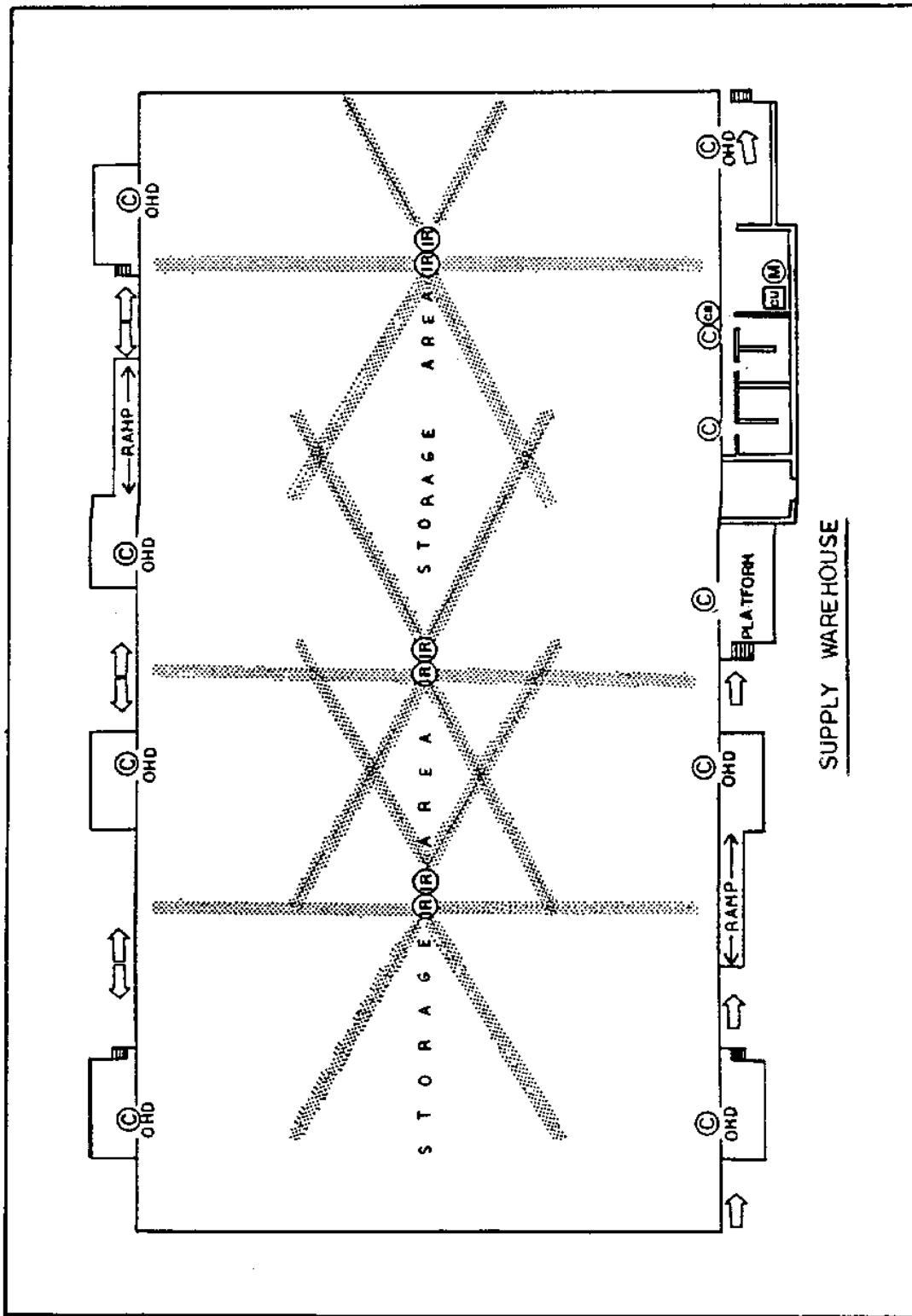


Figure 57
Supply Warehouse

9.5 Funds and Negotiable Instrument Storage Area. This facility IDS consists of detection and assessment subsystems (Figure 58).

9.5.1 Detection. The detection subsystem uses point and volumetric sensors to protect the perimeter and interior of the facility. The point sensors are balanced magnetic switches at perimeter doors and entry to areas storing high value assets. Interior sensors will avoid the need for perimeter glass breakage detection sensors. Passive infrared sensors are specified because of the open area environment that will contain items that are nuisances to microwave and ultrasonic phenomenology. The off-site reporting of the system will include at least one test per day of system communications.

9.5.2 Assessment. The assessment components are closed-circuit television cameras that permit remote monitoring at principal access points and immediately outside the secured funds storage area. Early assessment of alarm conditions are important to properly direct response forces to the source of alarms.

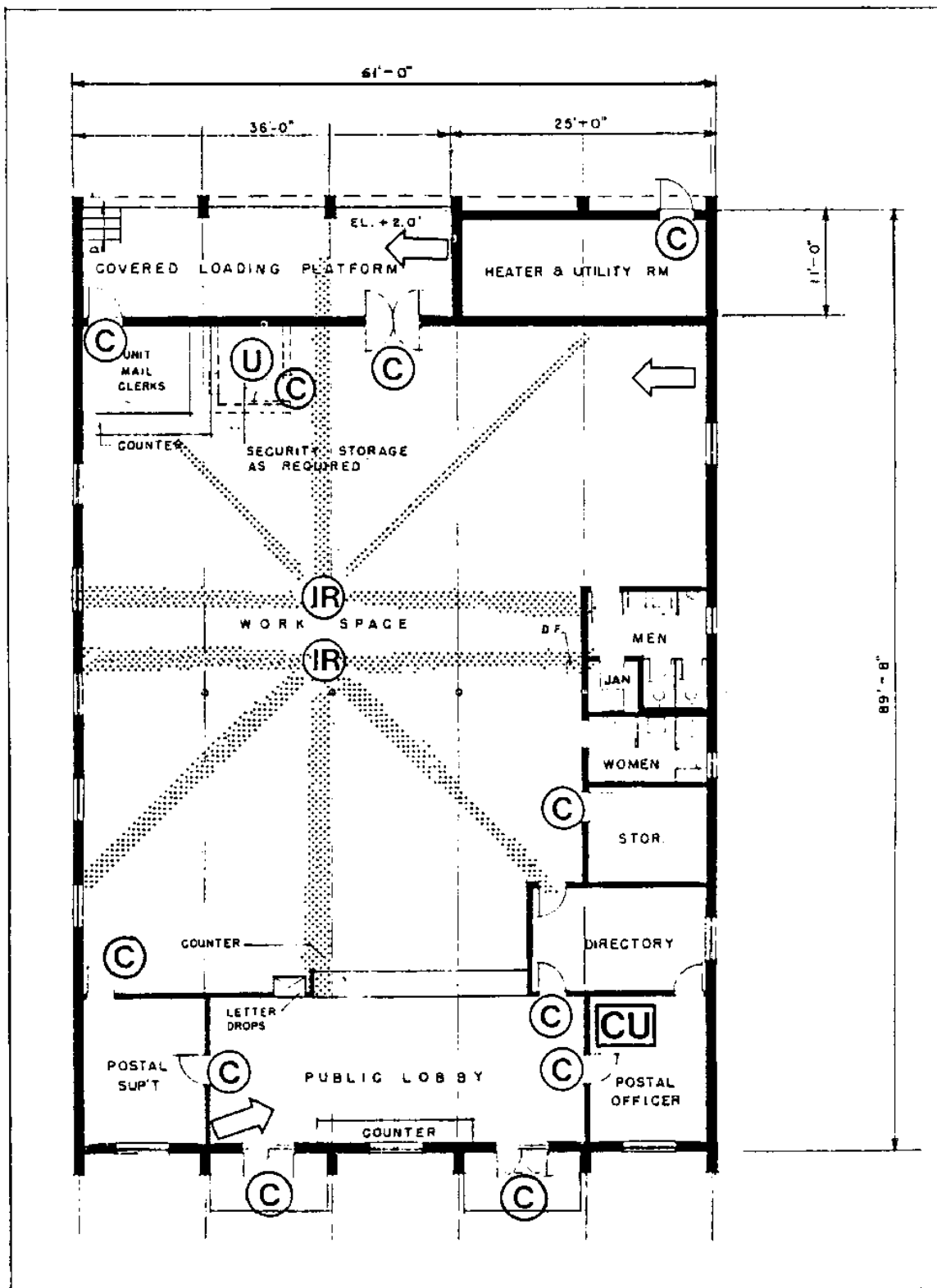


Figure 58
Funds and Negotiable Instrument Storage Area

9.6 Intrusion Detection System Monitoring Area. This facility IDS consists of a detection subsystem, an assessment subsystem, and an intercom (Figure 59).

9.6.1 Detection. The detection subsystem consists of balanced magnetic switches on the doors to detect unauthorized opening or operator propping open the door for ventilation. When the facility is closed to normal visitors and manned for monitoring, the BMS for intrusion detection will be placed in the secure mode at the control unit. Duress alarm switches are located within easy reach of the operator to permit off-site notification to response forces. These systems require a minimum of once per duty shift testing to ensure communication functions and operator confidence in the system. Closed-circuit television cameras provide continuous assessment of personnel approaching the facility. When interfaced with a video motion sensor, it will provide early warning to monitoring personnel of incoming personnel or vehicular traffic.

9.6.2 Assessment. CCTV monitors are located in both office and monitoring rooms to display pictures from exterior CCTV cameras. Intercommunication between the front door and monitoring room will allow for audible request for access to the station with assessment provided by the CCTV system. Upon verification of identification, the console operator can remotely open the front access point by activating an electric strike with a manual switch.

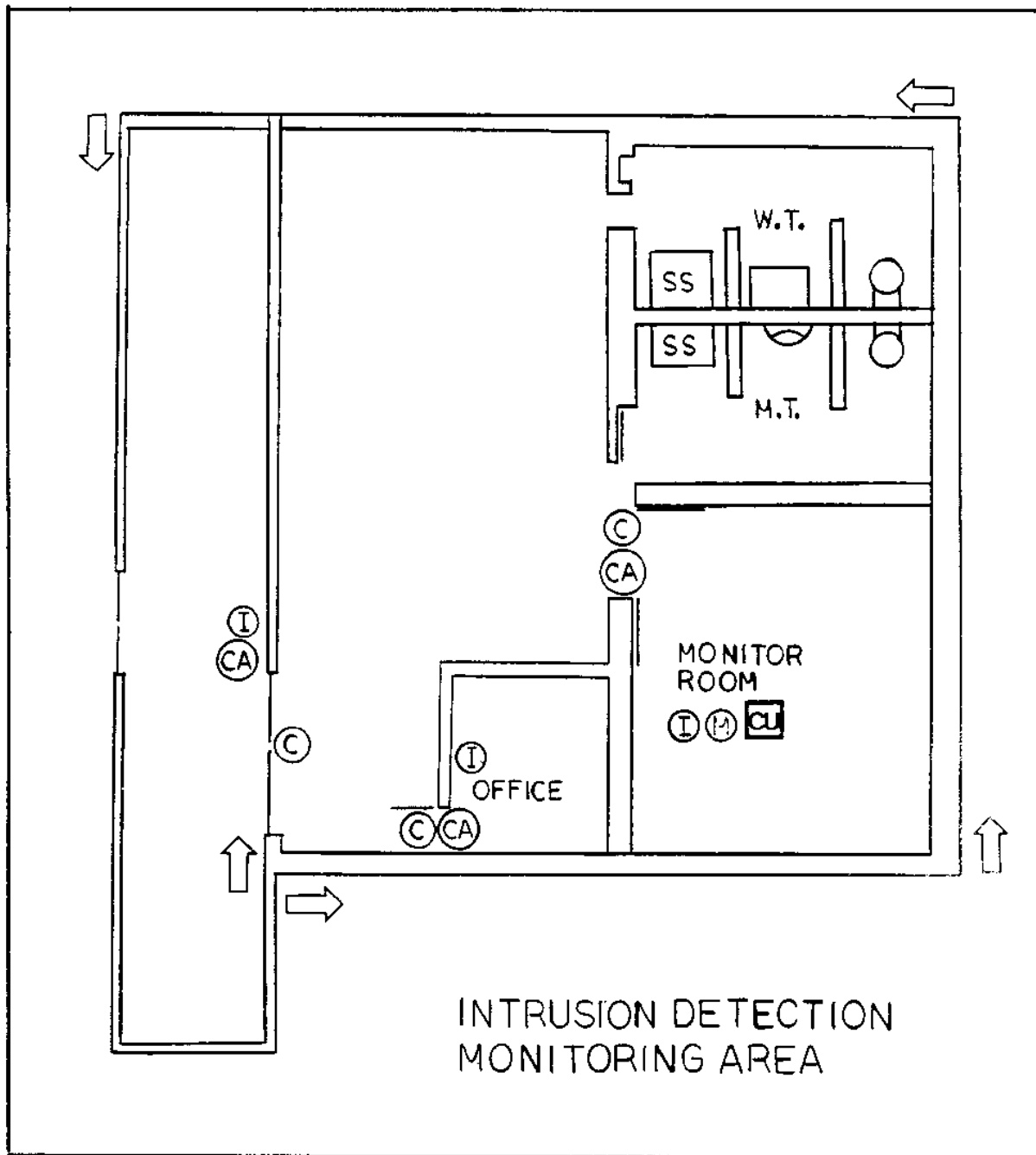


Figure 59
Intrusion Detection System Monitoring Area

9.7 BX Retail Area. This facility IDS is designed for use when each individual place of business is closed. Each place of business should have independent system control with a local annunciator and control unit (Figure 60).

9.7.1 Perimeter. The perimeter detection components consist of balanced magnetic switches on exterior doors to detect access to contiguous spaces.

9.7.2 Interior. The interior detection components consist of passive infrared motion sensors located to protect large open-space volumetric areas.

9.7.3 Control and Annunciation. The control components consist of a master control unit and individually located subcontrol units per business zone. Each zone will have a duress alarm switch initiation provision. Zones will be individually annunciated at the protected premises and at a remote location. The transmission of alarm information will be via supervised hardwire, cable, radio, or fiber optic communications. This data will include opening and closing reports. These reports will indicate each time the alarm system is armed and disarmed. When the opening or closing schedule is not met, an alarm will be generated and will require resolution by the monitoring personnel. In order for the entire facility protection to be effective, all detection components in each zone must be operating.

9.7.4 Assessment. The assessment subsystem consists of closed-circuit television cameras which view the approach to the protected perimeter in order to confirm the intrusion point or to assess individuals noted in the vicinity.

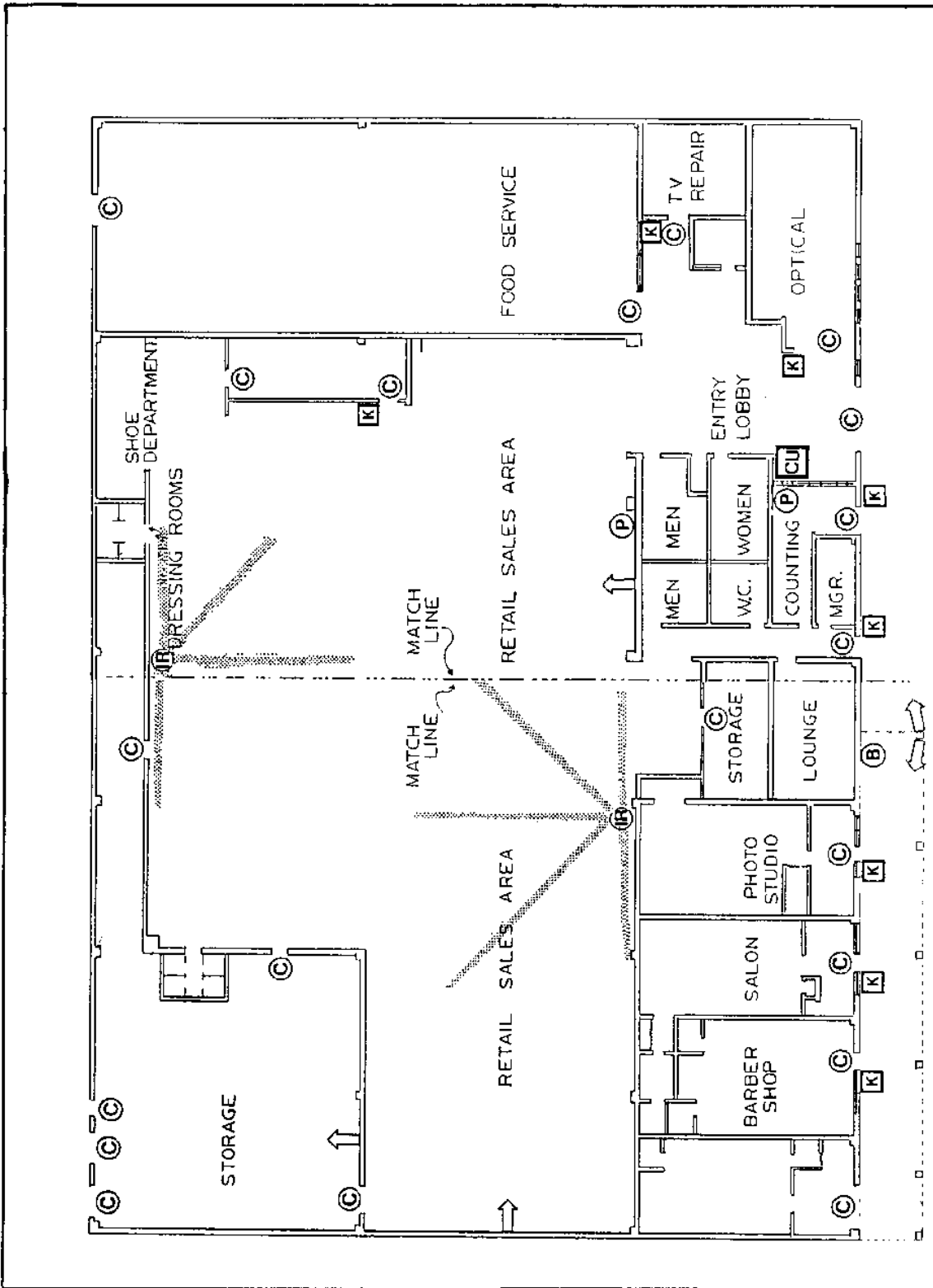


Figure 60
B.X. Retail Area

9.8 Commissary Retail Area. This facility IDS consists of detection and subsystems (Figure 61).

9.8.1 Detection. Alarm Reporting and Display Perimeter Detection components are comprised of balanced magnetic switches to detect intrusions at each exterior portal. Interior detection components are provided to detect intruders at the corridors which enable access to assets. This IDS is designed to detect stay-behind intruders and provide protection-in-depth.

9.8.2 Alarm Reporting and Display. The control unit permits arming and disarming of the IDS. The communications scheme utilizes telephone wiring connection to a central alarm reporting and display processor. The arm/disarm functions are monitored and compared to an opening/closing schedule with exceptions to the schedule treated as an alarm event. Duress alarm switches operate on a 24-hour basis and are located at cashier stations and within the counting room.

9.8.3 Assessment. Closed-circuit television assessment is not recommended for this facility since off-site monitoring of the after hours activity will not provide information of value to response force resolution of an alarm event.

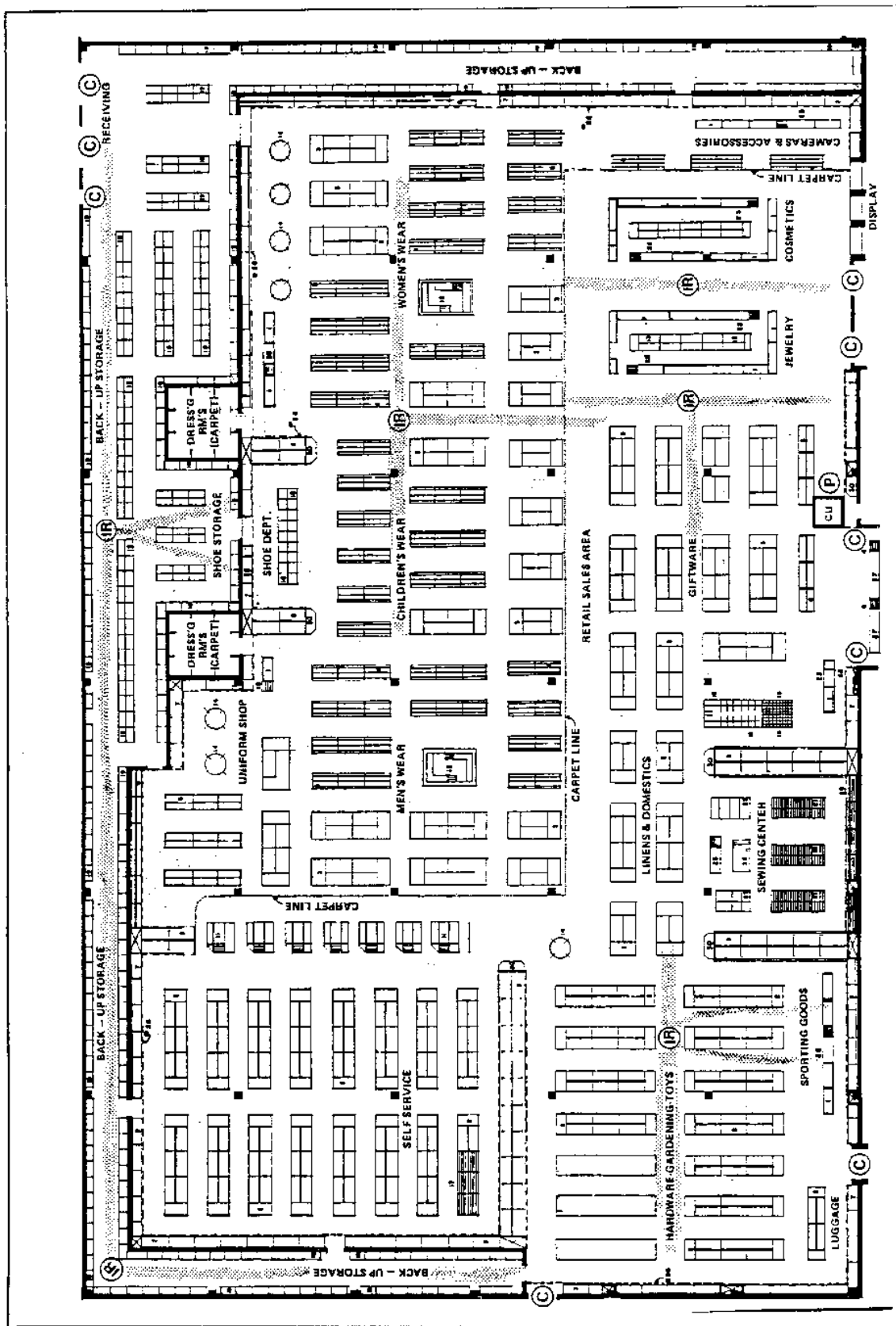


Figure 61
Commissary Retail Area

9.9 Command Quarters. These are residential IDS systems designed for use either when occupants are at home or away (Figure 62).

9.9.1 Detection. Perimeter components consist of balanced magnetic switches on exterior doors and windows. Interior components consist of passive infrared motion sensors located to protect valuable asset locations and the entry hallway. If the occupant lifestyle includes small children or pets, the motion detection scheme needs to be altered to permit more freedom within the protection zones if the entire system is armed. Alternatives to the extensive motion detection or interior traps will require either a full perimeter system (addition of glass breakage and wall penetration detectors) or limited selective use of curtain type infrared motion detectors.

9.9.2 Alarm Reporting and Display. The control components consist of a control unit and two key stations. The control unit will use four detection zones: perimeter, interior, delay (for entry and exit door), duress, and report alarms by hardwire telephone lines. The key station will permit selective arm/disarm and duress switch activation from the entry hallway and within the sleeping area.

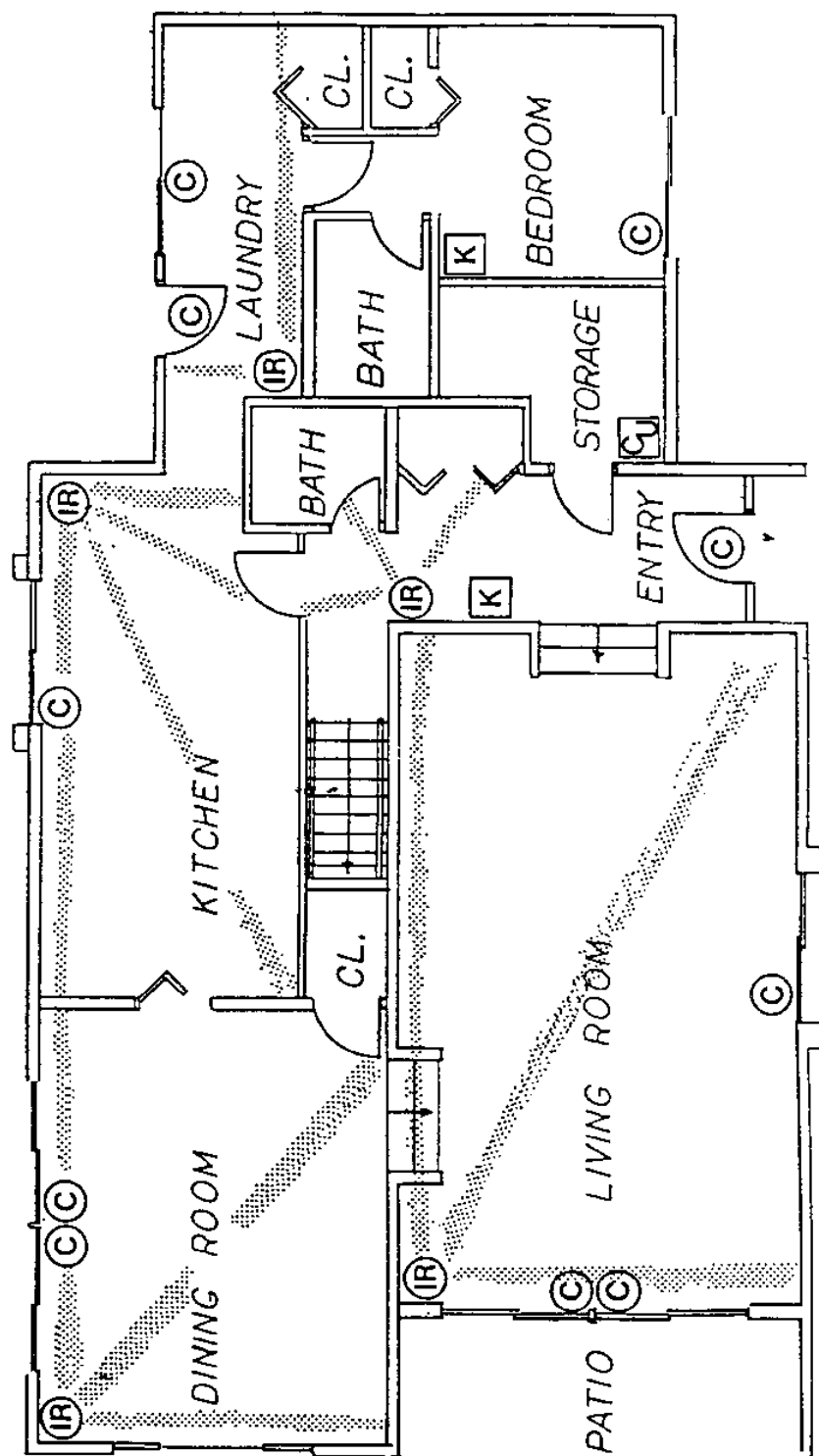


Figure 62
Command Quarters

9.10 Sensitive Compartmented Information Facility (SCIF). This facility IDS consists of automated access control, detection, and assessment subsystems (Figure 63).

9.10.1 Access Control. The access control components permit previously approved individuals to enter the protected area based upon "two-man" rule, time of day, anti-passback, and area loading criteria. The controlled access point for entry to the SCIF utilizes electronics on a day gate since excessive wear will result when a vault door is used for common entries. This day gate is denoted as the inward opening door. The access control components will report and store information on access attempts and denials and approvals but will not inhibit detection alarm reporting. Requirements outlined in directives indicate the need to cause an alarm each time an armed IDS area is entered. No disarming can occur from outside the protected area.

9.10.2 Detection. The detection components consist of point and volumetric sensors which will annunciate any intrusion into the protected area. The arm/disarm key station should be located within the protection of the IDS perimeter to avoid having any means to disable the system without causing an alarm. Also, delay timers to permit entry of the perimeter to disarm system without causing an alarm are not permitted. The IDS control output will require filtering.

9.10.3 Assessment. The assessment subsystem consists of closed-circuit television cameras located outside the protected perimeter and one intercom at the principal entrance. Cameras will permit egress or alarm verification. The intercom is a convenience device designed to permit communication between persons entering the facility and the remote monitoring site. Due to the classified storage vulnerabilities within the facility, cameras are not used within the facility to avoid the chance of compromise of classified data.

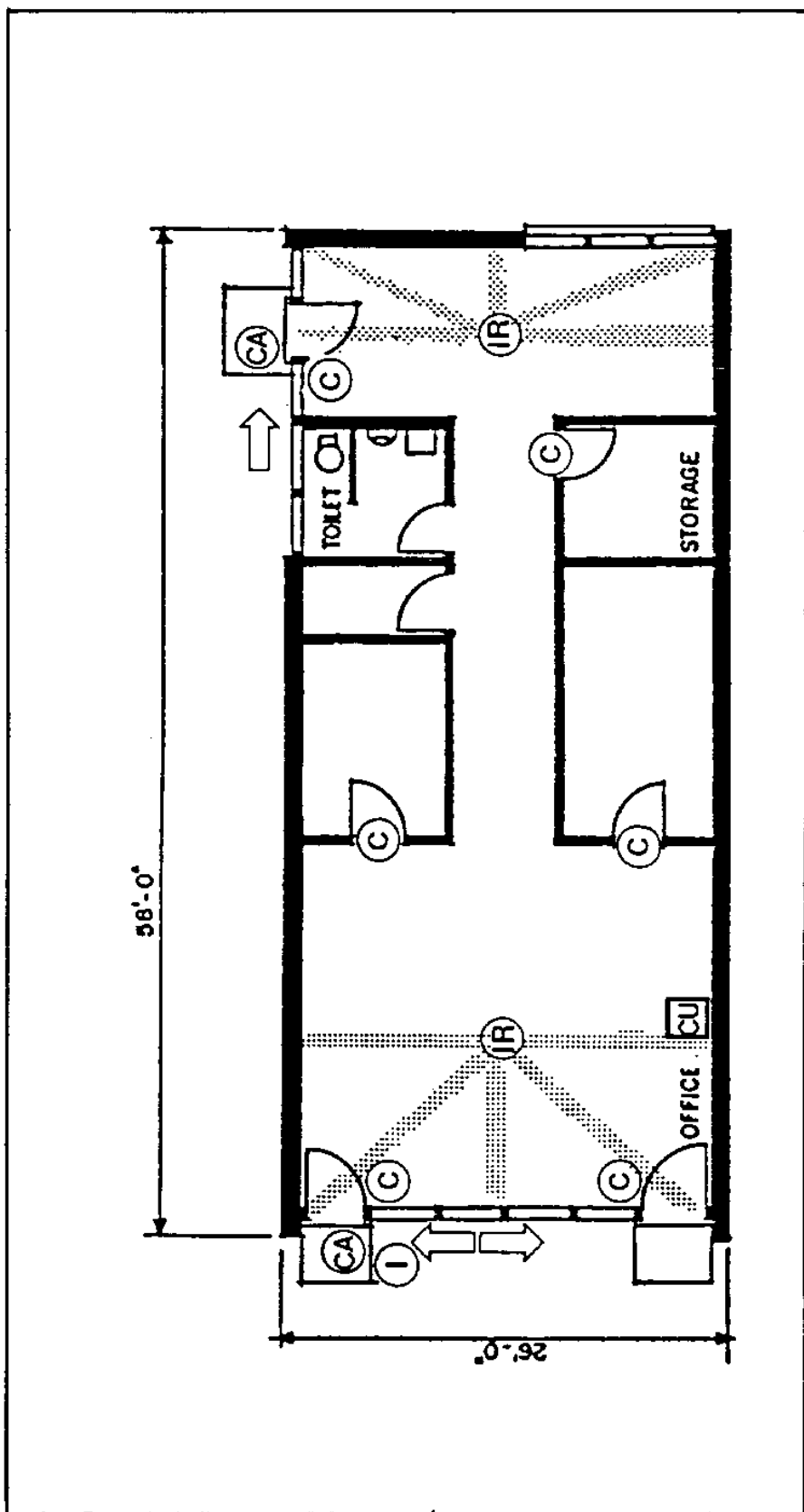


Figure 63
Sensitive Compartmented Information Facility (SCIF)

9.11 Navy and Marine Corps Reserve Facility. This facility IDS consists of two detection and alarm monitoring and control subsystems (Figure 64).

9.11.1 Detection. The detection subsystem consists of perimeter components consisting of infrared and supervised BMSs and interior components consisting of volumetric, passive infrared motion. Perimeter rooms with glass windows are equipped with passive infrared sensors. These sensors will provide detection of entry into the room from an interior door or through a broken window or wall. Infrared units located in the corridors are for detection of stay-behind intruders who may hide in spaces above the ceilings. BMSs will be installed on doors of rooms which contain valuable or high risk assets.

9.11.2 Alarm Reporting and Display. The control unit provided for multiple zones allows selective arming of areas within the facility and off-site reporting of alarm events. This will provide for securing certain sections of the facility while others are occupied. This type of facility may require local police department notification for resolution of alarm events since the reserve centers are often located outside the jurisdiction of Base police forces.

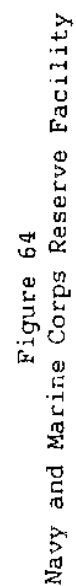


Figure 64

9.12 Training Facilities. This facility IDS consists of automated access control and detection and alarm reporting and display subsystems (Figure 65).

9.12.1 Access Control. The automated access control components will permit access to the vault by authorized persons. This subsystem is considered to be stand-alone since the access will only be permitted during duty hours when the complementary detection subsystem is disarmed.

9.12.2 Detection. The detection components are point and volumetric sensors protecting the entire perimeter and selected interior spaces. Balanced magnetic switches are used on exterior entry doors and glass breakage detectors in order to detect area-to-area movement of stay-behind intruders.

9.12.3 Alarm Reporting and Display. The reporting of alarms to remote monitoring personnel is a function of the control unit. This facility is considered to have specific duty hours that permit securing the entire perimeter after closing hours. The monitoring and reporting can be proprietary if this facility is part of a larger facility that is occupied on a 24-hour basis. Access control subsystems will permit routine patrols of the area and may be used as a record of these patrols.

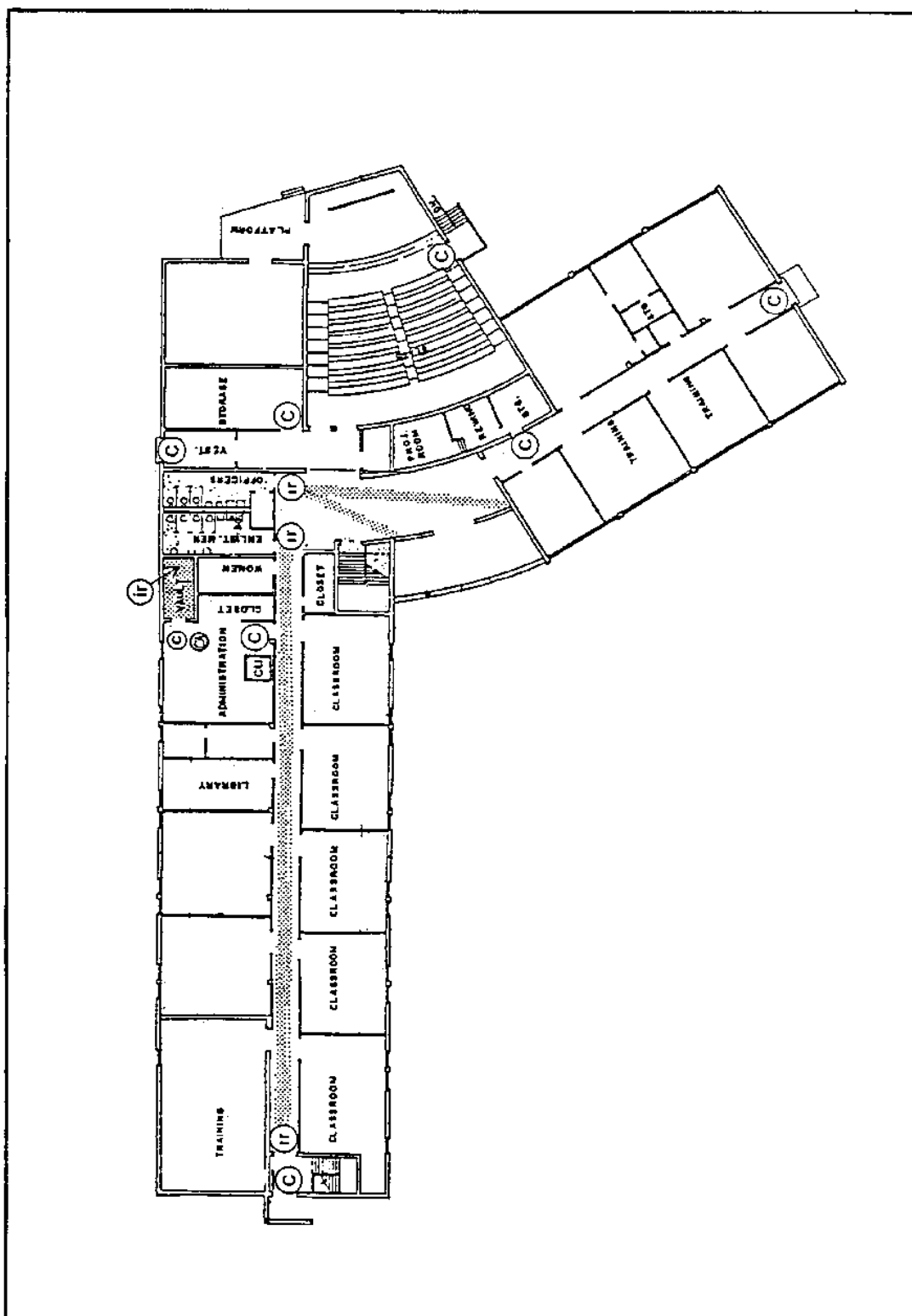


Figure 65
Training Facilities

9.13 Automated Data Processing Facility. This facility IDS consists of automated access control detection and assessment subsystems (Figure 66).

9.13.1 Access Control. The access control devices are card readers located at entry/exit portals that permit unlocking of doors based on authorized card holder, day of week, and time of day authorizations.

9.13.2 Detection. Balanced magnetic switches are used on each door to detect unauthorized opening or propping open of doors. The passive infrared motion detectors will detect stay-behind intruders when the system is armed for after duty hours. Access control and detection sensors report alarms and status exceptions to both off-site monitoring and local annunciators. This facility is considered to be a part-time use portion of a large facility. The system will use a proprietary reporting scheme. If equipment in computer area is processing "RED" data, the unexposed wiring connected to the underneath raised flooring (grounding plates, etc.) needs to have sensor placement to detect tampering.

9.13.3 Assessment. Closed-circuit television cameras are used to permit remote monitoring of the area after closing hours.

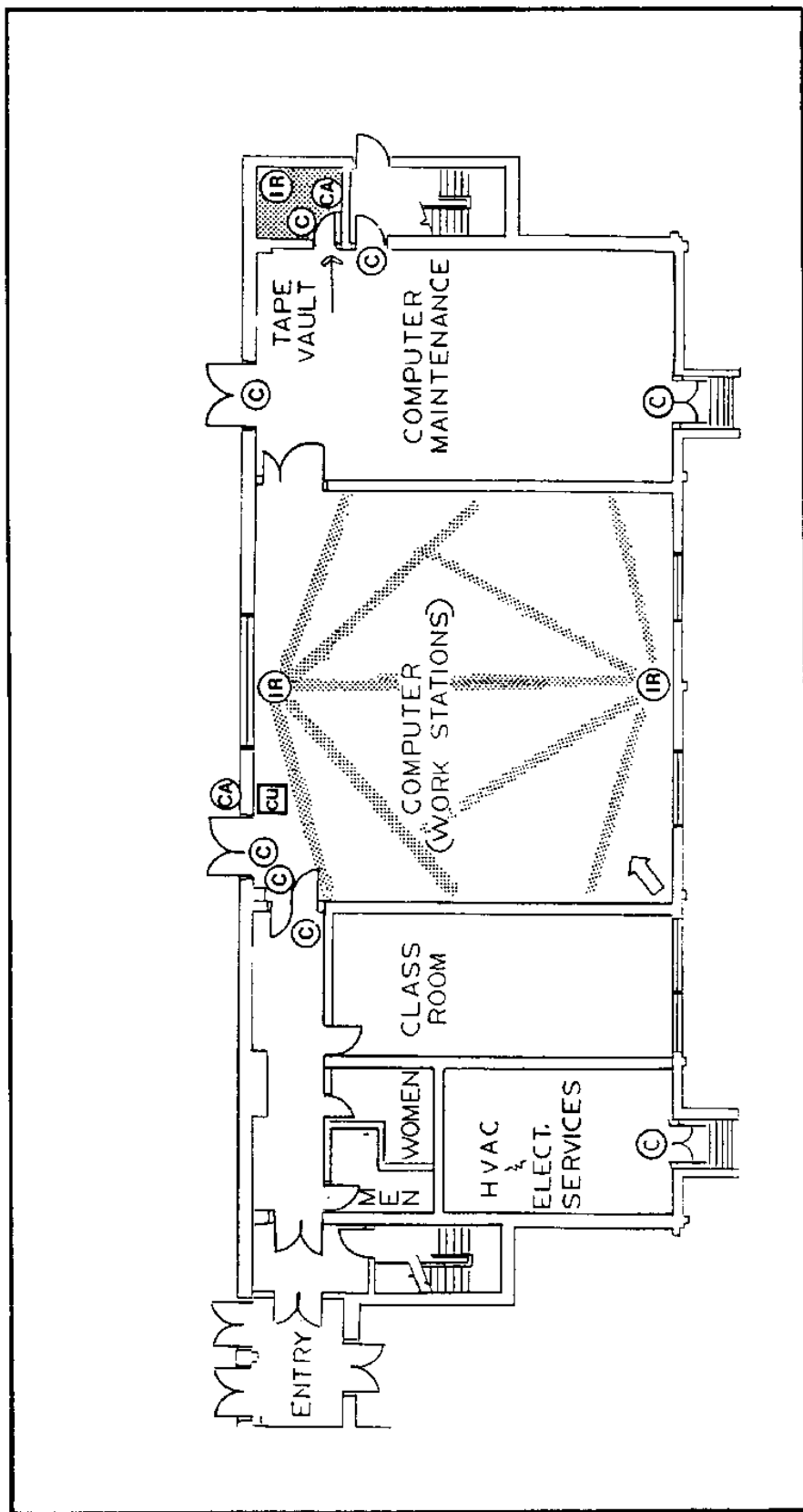


Figure 66
Automated Data Processing Facility/Area

Section 10: INTRUSION DETECTION SYSTEMS
SITE SURVEY GUIDE

10.1 Purpose. The purpose of this site survey guide is to provide a list of important items to be investigated during preliminary engineering and project design stages of NAVFAC projects which involve the integration of intrusion detection systems into the facility design process.

10.1.1 Classification of Completed Guides. Caution should be exercised by individuals performing the completion of these questions on sensitive projects. Specific responses to certain questions may be classified in themselves or in the aggregate. It is the responsibility of the project engineer to be thoroughly familiar with applicable security classification guides and to protect resultant classified information accordingly.

10.1.2 Relationship of Checklist to Applicable Directives. The questions incorporated in this guide are necessarily broad in scope due to the diverse range of applications potentially involving NAVFAC project tasking. Individuals assigned to the design and installation management of specific security system upgrade projects should review applicable DoD and Navy directives and refer to specific checklists which may be included therein. Examples may be found in OPNAVINST 5530.14, U.S. Navy Physical Security Manual, (Appendix III) and DIAM 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities (enclosure 5). The guidance contained in NAVFAC DM-13.01, Physical Security, may also be applicable in terms of physical security since barriers and locking hardware items are the first line of facility defense.

10.1.3 Project Complexity. Obviously, this checklist would not be completed in its entirety for a relatively simple application. By the same measure, it may be too general for the very large multipoint installations found increasingly in Navy facilities. The design team should use applicable directives and guidance noted above and elsewhere in this manual and add or delete specific categories in accordance with the specific requirements of each site.

10.2 Using This Guide in Conjunction With the Design Manual. This guide is intended to be used in conjunction with the design process set forth in Section 3 of the design manual. The information contained in a completed survey is the data required for input to the requirements analysis phase of the process. While the survey format needs to be adapted consistent with the needs of each site, the total documentation of conditions and influences present during the survey form the foundation of the security systems implementation process.

INTRUSION DETECTION SYSTEM SITE SURVEY

UNIT/ACTIVITY _____ NAVFAC PROJECT NO. _____

ADDRESS OF SITE _____

ROICC NAME _____ OICC NAME _____

ROICC TEL. NO. _____ OICC TEL. NO. _____

USER ACTIVITY/NAME OF C.O. _____ TEL. NO. _____

DATE(S) OF THIS SURVEY _____

NAME(S) OF SURVEY TEAM _____

THIS SURVEY IS FOR INCLUSION IN: (1) 35% DESIGN ()
(2) 60% DESIGN ()
(3) PRE-FINAL (90%) DESIGN ()
(4) FINAL (100%) DESIGN ()
(5) RETROFIT INSTALLATION ()
(6) OTHER: _____ ()

THIS SURVEY: COPY NO. _____ OF _____

PAGE NO. _____ OF _____

ATTACHMENTS _____ THROUGH _____

IF INFORMATION INCLUDED
IN THIS CHECKLIST IS
CLASSIFIED, INDICATE
REQUIRED GUIDANCE
HERE:

PART I

GENERAL BACKGROUND INFORMATION

GENERAL FACILITY DESCRIPTION/USE:

Name of facility_____

Location_____

(Attach map indicating location)

Gov't.

BUILDING OWNERSHIP: Owned () Leased () From_____

OTHER TENANTS? Yes () No () List indicating location and type of operation:_____

BUILDING CONSTRUCTION: (GENERAL DESCRIPTION)	THICKNESS/RESISTANCE TO PENETRATION
--	-------------------------------------

Basement Floor_____	_____
Upper Floors_____	_____
Walls_____	_____
Ceilings_____	_____
Interior Walls_____	_____
_____	_____

Date Constructed_____ By_____

Location of Plans and As-Built Drawings:_____

General Workmanship/Condition:_____

Near-Term Modifications Planned_____

Will Modifications Impact IDS?_____

Mission/purpose of facility:_____

Facility Sensitivity/Criticality:_____

Location(s) of critical functions/assets in rank order: (Indicate on floor plan)

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

13.02-157

THREAT SUMMARY

Generic Threats Inherent in Facility Mission/Function: _____
Describe man-made, _____
natural phenomena _____
potential for area or _____
accidental events _____
that have potential _____
for occurrence because _____
of the nature of this _____
facility. _____

Have facilities of this nature been victimized elsewhere in this region?
No () Yes () _____

If yes, explain cause/consequence. _____

Predictors of potential threats - current reports or intelligence that this
or similar facilities may be target of overt or covert activities: _____

Indicate capabilities of potential adversary groups/individuals: _____

Potential Threat Objectives on site: _____

Actual events at this location:

EVENT	DATE	CONSEQUENCES
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Comments: _____

SECURITY FUNCTION:

Responsibility for facility security: NAME:_____Tel. No._____

Total security complement:_____ Hours of coverage: From____ To:____

Complement each tour of duty:_____

Military security force () Civilian () Other_____

Supervision: _____

Training provided:_____

Turnover rate: _____

Selection criteria/qualification_____

_____Unionized?_____

Unionized? _____

Principal functions/responsibilities (in rank order):_____

No. of fixed posts:_____ No. of mobile/roving posts_____

Ancillary functions:_____

Written Procedures? Yes () No () Update Frequency_____

Limitations on new or revised functions:_____

Organizational unit(s) responsible for Electronic Sensor Maintenance:_____

If none available in-house, vendor(s) utilized:_____

Response time to call for service_____General capabilities:_____

Security Force Equipment:

Type

Quantity

Location

Comments: _____

13.02-159

PUBLIC AUTHORITY:

Name of agencies with local police power/jurisdiction:

AGENCY	LOCATION	COMPLEMENT	CONTACT
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

General Capabilities:_____

Accept Alarm Devices?_____

Response Time:_____

If agency contacted, what problems/needs did they observe for this site?_____

GENERAL SITE CHARACTERISTICS:

Population:_____ Type Local Government:_____

Demographics:_____

Principal local problems of impact on site:_____

Comments:_____

If activity is located on-base, is access to Navy property adequately controlled?_____

Is access to the site planned for security upgrade controlled?_____

If yes, what measures are used?_____

13.02-160

13.02-161

If portals are (or to be) manned, describe function of Entry Control Point (ECP) officer(s):_____

If portals are (or to be) covered by CCTV, describe viewing adequacy:_____

Each ECP has communications?_____

For manned or machine-aided portals, what are estimated throughput rates by peak period(s) of use? (Key to portal number designation)_____

Are electronic or procedural search aids (to be) employed? No () Yes ()
Describe:

What design requirements exist for the access control subsystem? (Check all features which apply)

Multiple Access Levels _____Fast Throughput _____ Area Authorization _____
Time Zoning _____ Occupant Listing _____ Multiman Control _____ Anti
Pass-back _____ Positive Personal Identification _____ Line Security _____
Expansion_____Capability _____ Other: _____

Describe barriers employed at each ECP, estimate penetration resistance:

Are employees badged? Yes () No () Visitors Yes () No ()
Visitor Sign-in? Yes () No ()

Are badges color or other-coded for classification? Yes () No () If yes,
describe method:_____

Controls employed for vehicle access to protected area(s):_____

Controls over blank badges? Yes () No () Describe:_____

Card access system used? Yes () No () Mfgr:_____

Mod. Type_____ Reader Type_____ No. portal locations:_____
(Indicate on floor plan) No. access levels_____

No. of holders/each level:_____

Designated emergency exits (indicate on floor plan)_____

Will multiman rules be employed? Yes () No () If yes, in which areas?_____

Describe entry/exit control procedures, expansion plans, current or anticipated problems, comments:_____

WINDOWS/UTILITY PORTALS: (Cover openings greater than 96 sq. in. where forcible entry is possible.)

[illegible]

THREAT LEVEL CONSIDERATION: Are key individuals or function located behind windows that are observable from the exterior of the facility?_____

KEY COMBINATION CONTROLS:

Are key and lock combination controls in place? Yes () No () If yes, describe:

When was the last visual key audit made? _____ By whom? _____

Have losses occurred with no forcible entry? _____

How often are locks and combinations changed? _____

Are keys recovered when issues leave? Yes () No () _____

Are duplicates (masters, etc.) stored securely? Yes () No () _____

Who has access? _____

Who/where is locksmith? _____

Comments: _____

SAFE/VAULTS:

LOCATION	ACCESS BY	PHYSICAL AND PROCEDURAL CONTROLS EMPLOYED	U.L./OTHER RATING	PENETRATION RESISTANCE

Contents (key to each above location): _____

How are inventories or counts made on assets: _____

Frequency? _____ Responsibility: _____

Shortage reported? _____

Resolution: _____

GENERAL INVENTORY (physical and procedural controls employed over other assets):

13.02-164

SECURITY LIGHTING: (Complete for areas where direct surveillance or CCTV assessment may be required.)

LOCATION	SECURITY OPERATIONAL REQUIREMENT(S)	TYPE	EFFECTIVENESS DISTRIBUTION	GLARE	PHOTOMETER READING

Is lighting on auxiliary power? Yes () No () Partial () _____

Frequency of Aux. Power Test: _____

How are lights controlled: Auto Timer () Photo Cell () Manual ()

Hours used: _____

How are controls secured? _____

Can lights be easily compromised? _____

Fixtures vandalproof? _____

Cost effectiveness: _____

POWER SUPPLY:

Who supplies power to site?_____

Location of nearest representative:_____

Where does power come onto site?_____

How can this primary source be incapacitated?_____

Type of primary power: Single Phase () 2 phase () 3 phase () 50Hz ()
60Hz () 110 V () 220V () Other () Specify _____

Is power stable? Yes () No () Spikes () Brownouts () Other_____

Cable Runs: Exposed () Conduit () Cable Trays () _____

Is there a source of emergency power on-site? Yes () No () If yes: Gas ()
Diesel () Battery () Combination:_____

Capacity:_____ Manufacturer:_____

Where located?_____

Fuel source:_____

Are these areas secured?_____

Does system provide uninterruptible power? Yes () No () If no, time to
full capacity:_____

What does system support?_____

Comments:_____

EXISTING TELECOMMUNICATIONS:

Telephone Lines enter building where?_____

Supplier:_____ Address:_____

Relay room location(s)_____

Relay room(s) secure?_____

Access controls: Yes () No () _____

Procedures for phone tech. access:_____

Number of instruments on site_____ Number of lines_____

Land Lines: Underground () Pole () Microwave ()

Data transmission in addition to voice? Yes () No () _____

Describe other on-site communications:_____

Is the telephone system proposed for alarm data communications from the protected area to the control point(s)? Yes () No () _____

If yes, will the control center be on-or off-site?_____

What is the condition/reliability of these telephone lines?_____

Will the use of these lines compromise facility security?_____

What security countermeasures are to be applied to these telecommunications?_____

If yes, what alternatives will be developed?_____

If dedicated lease lines will be used, can line costs be reliably predicted for the life of the proposed system? Yes () No () Source of cost data:_____

PAGE_____OF_____

PART II

SYSTEM DESIGN AND IMPLEMENTATION INFORMATION

GENERAL UPGRADE IMPLEMENTATION REQUIREMENTS:

What does management desire of their system?

<u>OPTIMUM</u>	<u>MINIMUM</u>

What threat level of protection is to be provided? _____

What regulations are applicable to the facility and equipment?

- _____ OPNAVINST 5530.14
- _____ OPNAVINST 5510.1F
- _____ OPNAVINST 5430.48A
- _____ UL 611, Central Station Burglar Alarm Units and Systems
- _____ UL 1076, Proprietary Burglar Alarm System Units (Mux Systems)
- _____ Federal Specification W-A-00450B (GSA-FSS)
- _____ NACSIM 5203, National COMSEC Information Memorandum
- _____ DIAM 50-3, Security Alarm Systems
- _____ CSP-1, Cryptographic Security Policies and Procedures
- _____ NFPA 70 National Electrical Code
- _____
- _____
- _____
- _____
- _____
- _____

Comments: _____

What groups and which people will be involved in the design and installation of the system?

Who

_____ NAVFAC Representative _____
 _____ Security Management _____
 _____ Operations Personnel _____
 _____ Technical Security Personnel _____
 _____ Public Works Personnel _____
 _____ Safety Personnel _____
 _____ Activity Command Personnel _____
 _____ Outside Contractors/Consultants _____
 _____ Others (list) _____

Will the following areas of expertise be represented in the design/installation group? Who will provide the expertise?

Who

_____ Familiarity with applicable regulations _____
 _____ Experience with local procedures _____
 _____ Labor and personnel representatives _____
 _____ Electrical/instrumentation engineers/technicians _____

_____ Knowledge of required IDS equipment capabilities and limitations _____

_____ Construction contractors _____
 _____ Budgetary Control _____

PROCUREMENT:

How will equipment and related system improvements be acquired? Competitive Bid () Sole Source () Turnkey () Built in-house () Other ()

If competitive, how chosen? Low Bid () Prior Experience () Best Design and Equipment () Other () _____

If sole source, what basis? On Approved List () Compatibility with present system () Other () _____

Are there any vendors or hardware that will not be considered? Yes ()

No () _____

Is J-SIIDS, FIDS, or other Tri-Service equipment required? _____

Comments:

EXISTING ALARM SYSTEMS (List systems currently in place)

Type	Location	Problems/Effectiveness
------	----------	------------------------

13.02-171

Rate the following factors according to their importance (e.g., 1-2-3-etc.) in designing and installing an alarm system:

_____ Initial cost	_____ Ease of maintenance
_____ Reliability	_____ Floor space requirements
_____ Ease of understanding how to operate the system	_____ Ease of reconfiguring or modifying
_____ Ease of physically operating the system	_____ Ease of expansion/modularity
_____ Response time	_____ Compatibility with existing or proposed procedures
_____ Amount of operator fatigue produced	_____ System listed in approved equipment catalog
_____ Amount of information which is presented	_____ Recommendations from others
_____ Ease of interpreting the information that is displayed	_____ Degree of line security
_____ Probability of detection	_____ Protection-in-depth
_____ Low false/nuisance alarm rate	_____ Equipment best satisfies technical requirements
_____ Ease of retrofit	_____ Low profile/cosmetics
	_____ Single/Multiple Operator(s)

Other:_____

Who will operate the system? _____

Who will maintain the system?_____

What constraints does this work force present?_____

What types of training aids will be required?

Printed Manuals_____

Lectures_____ Slides/Movies_____

Equipment/Operations demo. and practice_____

Familiarization_____

Factory/Vendor training_____

Who will conduct the training?_____

Is training budgeted?_____

How long?_____ Minimum_____ Maximum_____

Comments_____

13.02-172

NUISANCE ALARM CRITERIA:

INTERIOR:

AIR HUMIDITY

AIR TEMPERATURE

AIR VELOCITY

LOCALIZED HEATING

OBJECT MOVEMENT (+.025 METER/SEC.)

MOVEMENT OUTSIDE AREA

FLUORESCENT LIGHTING

LOOSE FITTING DOORS

MOUNT AREA VIBRATION

AMBIENT ACOUSTIC NOISE

RODENTS/ANIMALS

RFI

EMI

DUST

ELECTRICAL TRANSIENTS

ROTATING/MOVING MACHINERY

SEISMIC ACTIVITY

THUNDER/LIGHTNING

LIGHT MOVEMENT ACROSS AREA

OTHER

POTENTIAL PROBLEM AREAS ON-SITE
(indicate locations on floor plan)

EXTERIOR

Seasonal Temp. Extremes/Mo. Range

Surface Wind-Prev. Dir./Speed

Precipitation-Type/Avg. By Mo.

Visibility-Extremes/Duration

Cloud Cover-% by Day/Night

Severe Weather Extremes

Max. & Avg. Snowfall Depths

Soil Composition

Max. Expected Frost Depth

Extent of Sub-Sur. Strata to 1 Meter

Water Table Extremes/Variations

Terrain

Animals

Standing Water

Under/Overground Utilities

Other

ALARM COMMUNICATIONS:

Which data transmission techniques are most appropriate:

- _____ Point-to-point transmission (hardwire () microwave ())
- _____ Party-line multiplexing
- _____ TDM (Time Division Multiplexing)
- _____ FDM (Frequency Division Multiplexing)
- _____ Land lines
- _____ Radio links (Frequency Band(s))_____

If TDM will be used, have the following factors been considered:

- _____ Scan rate (i.e., frequency at which each input is transmitted)
- _____ Dead time and provisions for "remembering" information during this time
- _____ Effects of loss of synchronization and methods and time required to reestablish synchronization
- _____ Effects on assessment techniques

Are remote units needed for:

- _____ Sending control information to remote premises (e.g., to operate remote-controlled door strikes)
- _____ Exercising self-test features
- _____ Local annunciator for back-up purposes
- _____ Signal encryption/coding

Will the system use remote ACCESS/SECURE switches (i.e., premises control units (PCUs)) which must be operated by someone at the protected premises? _____

If PCUs will be used, consider the following:

For what reasons will PCUs be included in the system?

- _____ To meet regulations
- _____ Because PCUs are part of the manufacturer's system
- _____ To improve security by forcing a person to be at the protected premises
- _____ Other _____

Will an indication be provided in the Security Operations Center (SOC) whenever a PCU is switched from SECURE to ACCESS and vice versa?_____

Who will operate the PCUs?

- _____ Security personnel
- _____ Nonsecurity organization personnel responsible for the protected premises

What kind of line security will be used?

- _____ Protective measures such as conduit, burial, and concrete
- _____ DC (end-of-line resistor) supervision
- _____ Multiplexed or digital supervision
- _____ Data encryption

Why was this line security technique selected?

- _____ Only type available with the desired system
- _____ Compatibility with existing equipment
- _____ Equipment was listed in approved equipment catalog
- _____ Recommendations
- _____ Technical analysis showed this technique to be the best for the job
- _____ This technique was the least expensive
- _____ Other _____

ALARM SYSTEM DISPLAY:

What information does the console operator need when an alarm occurs?

- _____ Secure/access/alarm status of the zone
- _____ Geographic location of the zone
- _____ Time of the alarm
- _____ Supplementary text providing additional information such as special hazards or material associated with the zone
- _____ Instructions describing special actions to be taken
- _____ Telephone numbers of persons to call in emergencies
- _____ Maps of the secure area
- _____ Automatic CCTV coverage of the alarmed area
- _____ Other _____
- _____ Other _____

How are buildings and zones popularly designated at the facility?

- _____ By numbers only (e.g., Zone 4 or Building 838)
- _____ By letters (e.g., Q Site)
- _____ By full words (e.g., _____)

Comments: _____

What type of displays will be needed to present this information?

- _____ Annunciator panel with a readout for every alarm
- _____ Graphic (map or floor plan) annunciator display
- _____ Numeric readout with one readout for all alarms
- _____ Combination of annunciator panel for zones with numeric readout for areas within zones
- _____ Multiple numeric readouts
- _____ Lister printer (limited letter-number printout)
- _____ Teletype or typewriter printer (full message printout)
- _____ CRT display with limited letter-number display
- _____ CRT display with full message display
- _____ CRT display showing geographic map or floor plan
- _____ CCTV display of area which is alarming
- _____ Other _____
- _____ Other _____

How will the operator interact with the equipment?

- _____ Push buttons
- _____ Toggle switches
- _____ Function keyboard
- _____ Typewriter keyboard
- _____ Other (What?) _____

Where will microphones be located?

How will microphones be actuated?

- | | |
|-------------------------------------|----------------------------|
| _____ Built into the console | _____ Switch on console |
| _____ Desk-top stand | _____ Switch on microphone |
| _____ Suspended on adjustable mount | _____ Foot switch |
| _____ Part of headset | _____ Knee switch |
| _____ Telephone handset | _____ Cradle switch |
| _____ Other | _____ Voice actuated |

Comments: _____

ALARM SYSTEM OPERATIONS:

COMMUNICATIONS:

Using the listings below, identify communication requirements by drawing a line from each item in the left-hand column to every item in the right-hand column with which communication is required. Label each line with the type of communication which is used. For example, if the console operator reports alarms to a security officer via an intercom, draw a line from "console operator" to "security officer" and label it "intercom." Similarly, if a dispatcher communicates to a foot patrol by radio, draw a line from "dispatcher" to "foot patrol" and label it "radio." Some typical communication techniques are: face-to-face, intercom, dial telephone, direct-connect telephone, radio, teletype, and memorandum.

foot patrol	foot patrol
fixed post	fixed post
vehicle patrol	vehicle patrol
console operator	console operator
dispatcher	dispatcher
security officer	security officer
gate houses	gate houses
law authorities	law authorities
fire departments	fire departments
medical organizations	medical organizations
premises occupants	premises occupants
maintenance personnel	maintenance personnel
management	management
firstline supervisor	firstline supervisor
other:_____	other:_____
other:_____	other:_____
other:_____	other:_____

CONTROL CENTER LOCATION:

Where_____Size_____W_____L_____H_____

Wall/Floor/Ceiling construction_____

Bullet resistance requirement_____

13.02-177

Max. number operators req. _____

Will secondary alarm center be req.? Yes ____ No ____ Where located? _____

Complete redundancy req.? Yes ____ No ____ _____

Uninterruptible Power:

Will the system have a UPS Yes () No (). If yes, what type?

Diesel () Natural Gas () Propane () Battery () Combination ()

Other: _____

What components are supported by UPS? _____

Describe _____

How are power supplies physically secured? _____

Equipment Malfunction Considerations:

In general, how much of the system will be affected by the failure of a single component?

_____ Only one zone

_____ One module consisting of _____ zones

_____ Whole system

How will the system be checked for malfunctions?

_____ Periodic manual testing

_____ Use of self-test circuitry

_____ Use of lamp test circuitry

_____ Reliance upon line supervision or other fail-safe circuitry

_____ Other (_____)

What provisions will be made for periods of system failure?

_____ Emergency power (How many hours? _____)

_____ Redundant equipment operating in parallel at all times

_____ Redundant equipment, manually switched upon failure

_____ Manual procedures such as sealing areas, posting more guards, or increasing patrol frequency

Who will maintain the system?

- _____ Maintenance personnel from within the security organization
- _____ In-house maintenance personnel from another organization
- _____ Original equipment manufacturer
- _____ Outside service company
- _____ Other _____)

What technical skills will be required to maintain the system?

- _____ Basic electrical/electrician training
- _____ Electronics technician training
- _____ Computer hardware/logic circuitry technician
- _____ Computer software programmer
- _____ Electrical Engineer
- _____ Other _____)

Comments: _____



13.02-180

APPENDIX A

DESIGN SYMBOLOGY

The device symbol presents an easy to use and efficient means of identifying the essential features of the security engineering design effort. The symbol provides a method by which the phenomenology of the device, necessary identifying details related to the phenomenology of the device, and the means by which the device is positioned or mounted can be readily indicated on the engineering plans. The symbol also provides a means of identifying the device in order to develop accurate bills of materiel and system diagrams. The tables presented are suggested usage and can be modified as necessary to suit the particular design effort. The "completed Device Legend" is presented to illustrate actual devices and the legend detail needed on submitted plans.

Device Symbol:



Note:

- | | |
|--------------------|---|
| 1. Device Type | A single letter code used to indicate the phenomenology of the device. Refer to the device type list. |
| 2. Device Detail | A single letter code used to differentiate between similar type devices. Refer to the device detail list. |
| 3. Mounting Detail | A single letter code used to indicate the mounting means or positioning of the device. Refer to the mounting detail list. |
| 4. Identifier | Can be any alphanumeric sequence which allows identification of individual device. Room number with alpha character is particularly effective for interior plans which have specific room numbers previously assigned. |
| 5. Locator | Small (3/32 inch) dot which indicates the physical location of the device on the plans. Locator dot can be used with an arrow to indicate the location of directional devices, such as a CCTV camera, or with dashed lines to indicate fence mounted or buried line type devices. The symbol should be clarified in the legend and the plans. |
| 6. Symbol | A 1/2 inch or greater diameter circle with a horizontal line through the center. Can be changed to a square or hexagon of similar size, if necessary, for clarity on the drawings. The size is dictated by the height of letters used for the device nomenclature. |

2nd Letter - Sensor Detail

A	Ultracon
B	Intensified Silicon Intensified Target
C	Curtain
D	Vidicon
E	Angled left _ _Degrees (_ _Degrees from surface)
F	Reserved
G	Angled right _ _Degrees (_ _Degrees from surface)
H	Reserved
J	Reserved
K	Key pad
L	Long Range
M	Masked Coverage (Add Note to Legend & Spec for detail)
N	Reserved
P	Processor
R	Recessed
S	Surface
T	Transmitter
U	Receiver
V	Volume
W	Reserved
X	Reserved
Y	Reserved
Z	Reserved

1st Letter - Sensor Type (Phenomenology)

A	Acoustic
B	Balanced Magnetic Switch
C	Card Reader
D	Door Strike
E	Electrical Strain Sensitive
F	Fence Sensor
G	Glass Break
H	Reserved
J	Door Bolt
K	Capacitance
L	Photoelectric
M	Microwave
N	Radiation
P	Passive Infrared
R	Area Lighting
S	Switch (Contact)
T	Intercom
U	Ultrasonic
V	Video
W	Seismic (Vibration/Switchmat)
X	Ported Coaxial Cable
Y	Reserved
Z	Reserved

3rd Letter - Mounting Detail

A	Above Ceiling (above suspended ceiling)
B	Buried (Underground) (In pour or slab)
C	Ceiling Mounted
D	Duct Mounted
E	System Output to Control External Equipment
F	Flush Mounted
G	System Input from External Equipment
H	Header Mounted (above door opening)
J	Jamb Mounted (beside door opening)
K	Reserved
M	Reserved
N	Reserved
P	Pole Mounted (i.e., exterior CCTV)
R	Recessed Mounted
S	Surface Mounted
T	Table/Desk Mounted
U	Under Floor (below raised floor)
V	Reserved
W	Wall Mounted
X	Suspended
Y	Reserved
Z	Reserved

Completed Device Legend

ADT	X-Ray Unit Display Monitor Desk Mounted
ADE	X-Ray Video Source
BRH	Balanced Magnetic Switch, Recess Mount, Door Header
BSF	Balanced Magnetic Switch, Surface Mount in Floor
BSH	Balanced Magnetic Switch, Surface Mount at Door Header
BSP	Balanced Magnetic Switch, Surface Mount, on Post
BSJ	Balanced Magnetic Switch, Surface Mount in Jamb of Door
CKP	Card Reader with Keypad Post Mounted
CKW	Card Reader with Keypad Wall Mounted
CM	Control Monitoring Unit
CS	Control Station Used with Ultrasonic Sensors
CPU	Central Processing Unit
CXP	Card Reader without Keypad Post Mounted
CXW	Card Reader without Keypad, Wall Mounted
DRJ	Electric Door Strike Recessed Jamb Mounted
GYE	Ventilation System Butterfly Valve Output to Open Circuit in Equipment Supplied by Others
GYG	Ventilation System Butterfly Valve Input from Open Position Sensing Device
GZE	Ventilation System Butterfly Valve Output to Close Circuit in Equipment Supplied by Others
GZG	Ventilation System Butterfly Valve Input from Close Position Sensing Device
HYG	Ventilation Systems Blast Valve Input from Open Position Sensing Device
HZE	Ventilation System Blast Valve Output to Close Circuit
JSH	Door Bolt Locking Device, Surface Mount at Door Header
LTW	Active Infrared Transmitter, Wall Mounted
LUW	Active Infrared Receiver, Wall Mounted
MUS	Metal Detector Surface Mounted
NUS	Radiation Detector Surface Mounted
PCC	Passive Infrared, Curtain, Ceiling Mount
PCW	Passive Infrared Sensor, Curtain Detection; Wall Mounted
PMW	Passive Infrared Sensor, Masked; Detection to Left, Wall Mounted
PNW	Passive Infrared Sensor, Masked; Detection to Right, Wall Mounted
PVW	Passive Infrared Sensor, Volume Detection, Wall Mounted
RYE	Area Lighting Output to Energize Circuit in Equipment Supplied by Others
SRF	Switch Contact Recessed Floor Mounted
SRH	Switch Contact Recessed Header Mounted
SWG	Uninterruptible Power Supply Status Input from Sensing Device
SYE	Output Contact to Energize Door Open Circuit in Equipment Supplied by Others
SZE	Output Contact to Energize Door Close Circuit in Equipment Supplied by Others

Completed Device Legend (Cont)

TJT	Audio Communication Transceiver Table Top
TJW	Audio Communication Transceiver Wall Mounted
UEW	Ultrasonic Sensor, Detection Angled Left 75 Degrees (15 Degrees from Surface), Wall Mounted
UVC	Ultrasonic Sensor, Volume Detection, Ceiling Mounted
UVW	Ultrasonic Sensor, Volume Detection, Wall Mounted
VAC	Video, Ultracon Camera, Ceiling Mounted
VAP	Video, Ultracon Camera, Pedestal Mounted
VAW	Video, Ultracon Camera, Wall Mounted
VBP	Video, ISIT Camera, Pole Mounted
VDX	Video, Display Monitor, Console Mounted
VOC	Video, Vidicon Camera, Ceiling Mount
WYG	Potable Water Isolation Valve Input from Open Position Sensing Device
WZW	Potable Water Isolation Valve Output to Close Circuit in Equipment Supplied by Others
XPB	Ported Coax, Data Processor, Mounted in Buried Vault Enclosure
XWW	Ported Coax, Data Control Interface Unit, Wall Mounted
YTT	Keypad Unit, Stand Alone, Desk Mounted
ZTT	Personal Identity Verifier, Stand-Alone, Desk Mounted

BIBLIOGRAPHY

American Standard Practice for Protective Lighting. A85.1-1956 UDC 628.978, Illuminating Engineering Society, New York, New York, 1956.

American National Standard Practice for Roadway Lighting. ANSI/IES RP-8, Illuminating Engineering Society of North America, New York, New York, 1977.

Background and Information Related to the Security Upgrade of Conventional Arms, Ammunition, and Explosive Storage Structures, Gray, K. O., M-64-79-04, Civil Engineering Laboratory, Port Hueneme, California, 1979.

Double Fence Lighting for Maximum Security Institutions. DB 13024, Department of Public Works of Canada, 1974.

IES Lighting Handbook, Kaufman, J.E. (ed.), Illuminating Engineering Society of North America, New York, New York, 1981.

Imaging Subsystems Base and Installation Security System (BISS) Supplemental Report - IR Imaging, Doepel, F. T., Night Vision Laboratory, Fort Belvoir, Virginia, 1978.

Intrusion Detection Systems Handbook, SAND 76-0554, Information Systems Dept. 1730 Sandia Laboratories, Albuquerque, NM.

Let There Be Light, But Just Enough, Beardsley, C. W., IEEE Spectrum, Volume 12, No. 12, Institute of Electrical and Electronic Engineers, Inc., New York, New York, 1975.

Port Security Lighting: Dock and Harbour, Lyons, S. L., Vol. 61, No. 716, The Dock and Harbour Authority, London, England, 1980.

A Physical Security Requirements Assessment Methodology Definition, Feasibility, Assessment, and Development Plan, Pietrsak, L.M.; Caldwell, J. D.; Chamberlin, J.; Hawxhurst, J. P.; Sjovald, A., MRC-R-651, Mission Research Corporation, Santa Barbara, California, September, 1981.

Department of Defense activities may obtain copies of Design Manuals, P-Publications, and Definitive Drawings from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120. Department of Defense activities must use the Military Standard Requisitioning and Issue Procedure (MILSTRIP), using the stock control number obtained from NAVSUP Publication 2002.

Other Government agencies and commercial organizations may procure Design Manuals, P-Publications, and Definitive Drawings from the superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

Cryptographic Security Policies and Procedures, CSP-1, December 81.

DOD Ammunition and Explosives Safety Standards, DOD 5154.45, 1978.

Guidelines for Facility Design and Red/Black Installation, National COMSEC Information Manual (U), NACSIM 5203(C), June 82.

Information Security Program Regulation, DOD 5200.1-R, August 82, w/chngs.

Nuclear Weapons Security Manual (U), DOD 5210.41-M(C), March 9, 1983.

Nuclear Weapon Storage Facilities Handbook (Draft), May 1978.

Part 12, Joint Conventional Ammunition Security Policies and Procedures, DOD 5160.65.

Physical Protection of Security Interests. Draft, DOE Order 5632, September 83.

Physical Security Equipment: Assignment of Responsibility for Research, Engineering, Procurement, Installation and Maintenance, DOD 3224.3, December 1, 1976.

Physical Security of Sensitive Conventional AA&E at Contractor Facilities, DOD 5220.30, August 11, 1983.

Physical Security of Sensitive Conventional Arms, Ammunition & Explosives, DOD 5100.76-M, February 83, w/chngs.

Physical Security Standards for Sensitive Compartmented Information, DIAM 50-3, July 80, reprinted May 83.

Security Criteria and Standards for Protecting Nuclear Weapons, DOD 5210.41, September 12, 1978.

Security of Military Installations and Resources, DOD 5200.8, July 29, 1980.

Department of the Army, Commander, Army AG Publications Center, 2800 Eastern Boulevard, Baltimore, MD 21220.

AR 5-9	Intraservice Support Installation Area Coordination, 3 January 1978.
AR 15-15	Department of the Army Physical Security Review Board, 8 February 1977.
AR 50-5	Nuclear Surety Program, 1 September 1978.
AR 50-6	Chemical Surety Program, 15 December 1978.
AR 105-22	Telecommunication Requirements, Planning, Developing and Processing, 1 July 1978.
AR 190-10	Security of Government Officials, 2 October 1977.
AR 190-11	Physical Security of Arms, Ammunitions, and Explosives, 15 October 1981.

AR 190-13	Arms Physical Security Program, 23 August 1974.
AR 190-16	Physical Security, 15 March 1984.
AR 190-18	Physical Security of US Arms Museums, 19 July 1967.
AR 190-22	Search, Seizure and Disposition of Property, 12 June 1970.
AR 190-28	Use of Force by Personnel Engaged in Law Enforcement and Security Duties, 1 August 1980.
AR 190-30	Military Police Investigations, 1 June 1978.
AR 190-31	Department of the Army Crime Prevention Program, 1 January 1982.
AR 190-50	Physical Security for Storage of Controlled Medical Substances and Other Medically Sensitive Items, 4 March 1977.
AR 190-52	Countering Terrorism and Other Major Disruptions on Military Installations, 15 June 1978.
AR 190-51	Security of Army Property at Unit and Installation Level, 1 August 1978.
AR 190-54	Nuclear Reactor Security Program, 15 September 1980.
AR 195-2	Criminal Investigation Activities, 6 May 1977.
AR 380-5	Department of the Arms Information Security Program Regulation, 1 August 1983.
AR 380-40	Policy for Safeguarding and Controlling COMSEC Information, 1 June 1982.
AR 380-380	Automated System Security, 14 October 1977.
AR 381-10	US Arms Intelligence Activities, 15 February 1982.
AR 381-12	Subversion and Espionage Directed Against US Army and Deliberate Security Violations, 1 July 1981.
AR 381-14 (C)	Counterintelligence: Technical Surveillance Countermeasures (U), 26 November 1976.
AR 381-20	US Arms Counterintelligence Activities, 10 September 1975.
AR 530-1	Operations Security, 1 May 1978.
AR 530-2 (C)	Communications Security (U), 1 September 1982.

AR 530-3 (C)	Electronic Security (U), 15 January 1979.
AR 530-4 (S)	Control of Compromising Emanations (U), 15 August 1978.
AR 640-3	Identification Cards, Tags, and Badges, 15 May 1980.
DA PAM 190-52	Personnel Security Precautions Against Acts of Terrorism, 15 June 1978.
FM 19-30	Physical Security, 1 March 1979.
TB-5-6350-262	Selection and Application of Joint-Services Interior Intrusion Detection System (J-SIIDS).
TB-5-6350-265-1	Selection & Application Guide for Facility Intrusion Detection System (FIDS) Components, 23 March 1984.
TC 19-16	Countering Terrorism on US Army Installations, 25 April 1983.

Department of the Navy, Chief of Naval Operations, OPNAV Publications and Instructions, Washington, DC 20350 (Code OP-451).

OPNAVINST 5510.1G	Information Security Program Regulation, April 84.
OPNAVINST C5510.83E	Navy Nuclear Weapon Security Manual, 1982.
OPNAVINST 5510.45B	United States Navy Physical Security Manual, 1971.
OPNAVINST 5530.13	Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E), December 81 (Change no. 1, dtd. 12/20/83).
OPNAVINST 5530.14	U.S. Navy Physical Security Manual, June 1983.
OPNAVINST 5430.48A	Navy Security Manager Handbook, January 1979.
OPNAVINST 5239.1A	Automatic Data Processing Security Program, August 82.

Intrusion Detection Systems (IDS), NAVGAC Guide Specification NFGS-16727 (Draft).

Physical Security, NAVFAC Design Manual DM-13.01, March 1983.

Security Manager Handbook, Office of Naval Intelligence, December 1978.

NAVFAC Guide Specifications as required for security lighting, cabling, fence and other security elements to be included in proposed system designs.

Department of the Air Force, Air Force Publications Distribution Center,
Publications Distribution Office, Bolling Air Force Base, Washington, DC
20332.

AFR 125-37	The USAF Resources Protection Program.
AFR 205-1	Information Security Program, 7 December 1982.
AFR 205-11	Security Managers Guide, 1 December 1981.
AFR 207-1 (C)	The Air Force Physical Security Program (U), 9 November 1979, w/chngs.

Sandia National Laboratories (SNL), 1730 Sandia National Laboratories,
Albuquerque, New Mexico, 87185

Intrusion Detection Systems Handbook, Sandia National Laboratories, (SNL)
76-0554, 1980.

Barrier Technology Handbook, 77-0777, 1981.

Entry-Control System Handbook, 77-1033, September 1980.

Safeguards Control and Communications Systems Handbook, 78-1785, May 1979.

National Fire Protection Association (NFPA), Inc., Batterymarch Park,
Quincy, MA 02269.

70-84	National Electrical Code
493-78	Intrinsically Safe Apparatus

REFERENCES

The following publications may be obtained from: Department of the Navy, Chief of Naval Operations, OPNAV Publications and Instructions, Washington, DC 20350 (Code OP-451).

OPNAVINST 5239.1A	Automatic Data Processing Security Program (Apr. 85)
OPNAVINST 5430.48A	A Navy Security Manager Handbook (Jan 79)
OPNAVINST 5510.1G	Information Security Program Regulation (Apr 84)
OPNAVINST 5530.13	Physical Security Instruction for Sensitive Conventional Arms, Ammunition and Explosives (AA&E) (Dec 81 and change 1 of 12/20/83)
OPNAVINST 5530.14A	U.S. Physical Security and Loss Protection Manual (Sep 85)
OPNAVINST 5530.15	Marine Corps Physical Security
DM-4.03	Electrical Engineering, Switchgear and Relaying (Dec 79)
DM-4.06	Electrical Engineering, Lighting and Cathodic Protection (Dec 79)
DM-4.07	Electrical Engineering, Wire Communication and Signal Systems (Dec 79)
DM-13.01	Physical Security (Mar 83)

The following publication may be obtained from: Commanding Officer, Naval Intelligence Command, Washington, DC 20350, Attn: NIC-34

DIA 50-3	Physical Security Standards for Sensitive Compartmented Information facilities (May 80, reprinted May 83)
----------	---

The following publication may be obtained from: Director, U.S. Navy Communications Security Material Systems (CMSC), 3801 Nebraska Avenue, NW, Washington, DC 20390

(NACSIM) 5203	Guidelines for Facility Design and Red/Black Installation, National COMSEC Information Memorandum (C) (Jun 82)
---------------	--

The following publication may be obtained from: Information Systems Dept.,
1730 Sandia National Laboratories, Albuquerque, NM

SAND 76-0554

Intrusion Detection Systems Handbook

Department of Defense activities may obtain copies of Design Manuals, P-Publications, and Definitive Drawings from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120. Department of Defense activities must use the Military Standard Requisitioning and Issue Procedure (MILSTRIP), using the stock control number obtained from NAVSUP Publication 2002.

Other Government agencies and commercial organizations may procure Design Manuals, P-Publications, and Definitive Drawings from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

CSP-1	Cryptographic Security Policies and Procedures (Dec 81)
D)D 5200.1-R	Information Security Program Regulation (Aug 82)
NAVSEAINST C9210.22A	Requirements for Security and Safety of Nuclear Reactor Plants, Fuel and Components Containing Plutonium or Enriched Uranium (C)
NFGS-16727	Intrusion Detection Systems (IDS) (Dec 85)
Fed. Spec. W-A-00450B	Alarm Systems, Interior, Security, Components for
Mil. Std. 1472B	Noise Limits for Army Materiel

The following publication may be obtained from: National Fire Protection Association (NFPA), Inc., Batterymarch Park, Quincy, MA 02269

70-84

National Electrical Code

The following publications may be obtained from: Underwriters Laboratories (UL) Inc., 333 Pfingsten Road, Northbrook, IL 60062

UL 611-85

Central - Station Burglar - Alarm Systems

UL 1076-82

Proprietary Burglar Alarm Units and Systems

13.02-194